Data Protection Policy

Owner: Juniper Education

Version: 5.0

Date: 01/11/2024

Juniper

Contents

Data Protection Policy

Policy Statement

Juniper Education ("Juniper") is committed to compliance with all relevant data protection legislation. It will maintain a suite of policy documents setting out how it intends to implement management controls sufficient to ensure legal compliance with data protection legislation and will ensure that these documents are reviewed periodically to

a) test their adequacy in meeting the legal standards as they change over time, and

b) to test Juniper's compliance with them.

Aim

This Policy sets out the commitment and approach to compliance with data protection legislation by Juniper. It describes Juniper's approach to complying with its legal responsibilities set out in the Data protection legislation and how it enables individual rights to be upheld and exercised.

The policy is supported by a toolkit of templates, forms, checklists and other resources to support the management of data protection compliance.

Objectives

This Policy provides

- a clear frame of reference to determine the organisation's standards, aims, and ideals in respect of data protection compliance;

- information for interested parties including data subjects, data processors, and the regulatory authorities about how the organisation approaches data protection compliance;

Juniper will ensure that

- all relevant personnel and/or other persons it commissions to process personal data on its behalf have received appropriate and sufficient training in the application of its policies,
- sufficient and appropriate resources are available to ensure that it meets both its legal obligations in respect of data protection legislation and the standards that it sets through its policies,
- it works within prescribed data protection principles and will implement sufficient controls to ensure that it is able to demonstrate compliance with the data protection legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities,
- it upholds the rights and freedoms of people conferred on them by the data protection legislation, and
- those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people, and
- that it has sufficient controls in place to assist people who wish to exercise their rights.

Scope

This policy applies to all Juniper activities or operations which involve the processing of personal data.

This policy applies to anyone who is engaged to process personal data for or on behalf of Juniper including: employees, contractors, casual and temporary staff, directors and officers, and third-parties such as sub-contractors and suppliers, and anyone who Juniper shares or discloses personal data with/to. It also applies where Juniper is a controller or where it acts as a data processor for another data controller.

Legislation

Juniper has a head office in the United Kingdom and is regulated principally by the United Kingdom General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("the Act") and overseen by the UK Supervisory Authority, the Information Commissioner's Office ("ICO").

Other laws inter-relate with the Act and the UK GDPR including but not limited to the Privacy and Electronic Communications Regulations (2003) ("PECR") and the Freedom of Information Act (2000).

Juniper is established in the European Economic Area ("EEA") and is further regulated by the European General Data Protection Regulation ("EU GDPR") and the Protection of Personal Data Act 2002 and overseen by the Bulgarian Supervisory Authority, the Commission for Personal Data Protection ("CPDP").

Data Protection Officer (DPO)

Juniper has designated a Data Protection Officer issued with a job specification formally detailing their key functions and responsibilities.

The DPO shall ensure that their details are recorded on the Register of Fee Payers maintained by the Information Commissioner's Office (ICO) and that their contact details are provided to data subjects and maintained in relevant documentation. The DPO can be contacted at DPO@junipereducation.org

Fair Lawful and Transparent processing

The processing of all personal data by Juniper will only be undertaken in a *fair, lawful* and *transparent* manner meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data is being collected and to the people who the data is about if personal data is collected from sources other than the data subject. All privacy information and any changes to privacy information must be approved by the DPO.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful basis for the data processing activities intended to be applied to the personal data. The DPO is responsible for determining the lawful grounds for processing. Where the lawful grounds are consent, the consent policy will apply. Where the lawful grounds are legitimate interests a legitimate interests assessment (LIA) will be undertaken and documented. Where the lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in Juniper, a public interests assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented.

Each Process Owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control, that the consent policy is adhered to and a LIA/PIA is properly undertaken where necessary. The DPO will provide advice regarding lawful processing conditions and maintain a register of the lawful grounds for all of Juniper's processing activities involving the processing of personal data.

Transparency – Juniper will endeavour to provide sufficient information about how personal data is being processed to enable sufficient transparency about its handling of personal data. The DPO shall periodically review the apparent transparency.

Data processing purposes

Personal data shall only be collected, created or otherwise obtained for specific, explicit and legitimate purposes. No data processing shall be undertaken or commissioned without the approval of the DPO who shall maintain a record of processing activities (RoPA) and their purpose. Process Owners are responsible for ensuring that all of the data processing activities that they undertake and/or commission are logged in the RoPA and have been approved by the DPO. No personal data shall be used for any purpose other than that which it was collected and/or created for.

Data minimisation

Juniper will use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects. Process Owners are responsible for ensuring that no unnecessary, irrelevant or unjustifiable personal data is collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The DPO will provide advice regarding the justification of personal data collected or created.

Data accuracy

Juniper recognises that the accuracy of data is important and will use reasonable endeavours to ensure data is as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

Process Owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained accurate and up-to-date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up-to-date are treated appropriately through erasure or anonymisation. The DPO will provide advice regarding data accuracy.

Data retention

Juniper will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymisation.

Process Owners are responsible for determining the retention period for personal data under their control or sphere of influence and the DPO shall maintain a data retention schedule setting out approved retention periods and end of life treatment. The retention periods for personal data must be approved by the DPO. Because data retention is a vitally important issue as both the over-retention and under-retention of personal data could have a detrimental impact on both the data subject and Juniper, the DPO will undertake periodic data retention audits.

Information security

Juniper will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Children's data

Special measures will be taken by Juniper if processing personal data relating to including the nature of privacy information provided and approach to information rights requests.

If Juniper provides information society services (digital services) that might the used by people under the age of 18, the Process Owner shall consider the applicability of the Age Appropriate Design Code of Practice and make provisions accordingly.

Personal data relating to criminal convictions and offences

If Juniper is processing personal data relating to criminal convictions and offences it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

Special categories of personal data

Special categories of personal data reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation.

Juniper shall not process special categories of personal data unless it is necessary. Where the processing of special categories of personal data is necessary, the DPO shall ensure that the lawful grounds for such processing are documented and shall maintain a periodic review of the necessity to processing the special categories of personal data.

Consent

Juniper will interpret consent as defined in the GDPR and any consent shall not be valid unless:

- there is a genuine choice of whether or not to consent;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through a statement made by the data subject or by a clear affirmative action undertaken by them;
- Juniper can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent;

Juniper recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. Juniper recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

Where consent is the lawful basis for processing, the Process Owner shall ensure that consent is properly obtained in accordance with the conditions above.

Record keeping and accountability

In order to fulfil its responsibility to be able to demonstrate compliance with data protection legislation as well as in support of the policy on transparency Juniper will maintain records of the processing activities that it controls, undertakes or otherwise commissions ("RoPAs") as required by the Data protection legislation and specifically those required in Article 30 of the GDPR.

The DPO shall be responsible for providing records to the Information Commissioner's Office on demand as required.

Juniper shall strive to maintain additional documentation capable of demonstrating accountability as necessary. The DPO shall be responsible for determining what records should be kept, for how long and in what format in order to support its accountability.

Information rights policy

Juniper recognises the legal rights of those whose data it processes or intends to process and will ensure that appropriate information is provided advising them of their rights, and that policies and procedures are maintained to ensure that Juniper is able to recognise information rights requests and handle them appropriately when they are exercised. These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about Juniper's processing of personal data and the right to a judicial remedy and compensation

The Handling Data Subjects/ Information/Rights Request procedure sets out how information rights requests are to be handled and ensure that all relevant people are made aware of it.

Data Breaches

The DPO shall be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

All employees and individuals with access to personal data for which Juniper is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach.

Juniper will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches.

The Personal Data Breach Reporting Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and media about a

personal data breach.

Data Processors

Juniper reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors may be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data protection legislation.

Any member of Juniper wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The DPO shall provide advice and guidance in respect of this.

A written agreement shall be implemented between Juniper and the data processor which at least meets the requirements of the data protection legislation. The DPO shall ensure that a register of such agreements/arrangements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

No employee is permitted to commission or appoint a third party to process data on behalf of Juniper without adhering to this policy.

The Procedure for Appointing Data Processors sets out responsibilities, decision-making criteria and processes for appointing new data processors.

Data sharing, disclosure and transfer

Juniper will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the data protection legislation being in place. Data sharing agreements must be approved by the DPO who will maintain a register of all such agreements. Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data. This policy extends to appointing others to process personal data on our behalf, sharing personal data with organisations, and providing information to ad-hoc requests for information such as those which may be received from the police and other authorities.

Juniper will provide information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action may be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing by the DPO.

Internationalisation of personal data

Juniper will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom or EEA without the conditions laid down in the data protection legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that Juniper undertakes or commissions whether directly or indirectly must be approved by the DPO and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
- The territory into which the data are being transferred is within the EEA;

- The territory into which the data are being transferred has an adequacy decision issued by the European Commission and/or by the Information Commissioner;
- The transfer is made under the unaltered terms of the standard contractual clauses issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the European Commission;
- The transfer is made in accordance with one of the exceptions set out in the Data protection legislation.

Where necessary the DPO shall ensure that a risk assessment is carried out on any third country Juniper intends to transfer personal data to and that any supplementary measures are implemented as necessary to ensure adequate protection of personal data.

Risk assessment

Juniper will adopt a risk-based approach to processing personal data ensuring that it assesses any risks to privacy or to the rights and freedoms of people before commencing or commissioning or changing data processing activities. Where necessary it shall, as a minimum, ensure that a data protection impact assessment (DPIA) is undertaken where required by data protection legislation and/or when one is deemed to be desirable by the DPO.

Juniper will maintain a procedure setting out how data protection impact assessments are to be carried out and documented and ensure that appropriate resources are available to advise on DPIAs.

The DPO is responsible for maintaining a register of data protection impact assessments that have been undertaken by Juniper and for its periodic review.

Training and awareness

Juniper will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically. Process Owners shall determine the training needs of those people within their sphere of control and ensure appropriate data protection awareness and training is provided, measured and reported.

Continuous Improvement, audit and compliance checking

Juniper will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where no-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The Board of Directors will be provided with a summary of audit findings periodically.

Data protection by design and by default

Juniper shall strive to foster a culture of data protection by design and default. It shall ensure that measures are in place to encourage those involved in data processing activities to adopt a model of continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into processing activities.

Juniper as a data processor

Where Juniper acts as a data processor on behalf of a data controller (client), Juniper and the client will comply with all applicable requirements of the data protection legislation for so long as and to the extent that they apply to Juniper and the client.

Juniper and the client acknowledge that for the purposes of the data protection legislation, the client is the data controller and Juniper is the data processor.

The client will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to Juniper for the duration and purposes of the contract.

Juniper shall, in relation to any personal data processed in connection with the performance of its obligations under the contract:

- process that personal data only on the documented written instructions of the client unless Juniper is required by applicable laws to otherwise process that personal data. Where Juniper is relying on applicable laws as the basis for processing personal data, Juniper shall promptly notify the client of this before performing the processing required by the applicable laws unless those applicable laws prohibit Juniper from so notifying the client.

- ensure that it has in place appropriate technical and organisational measures, which should be reviewed by the client, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

- ensure that all personnel who have access to and/or process personal data are obliged to keep the personal data confidential and in relation to Juniper employees, in accordance with the terms of their employment; and

- will not transfer any personal data outside of the EEA unless the client consents to Juniper transferring personal data outside of the EEA or providing the following conditions are fulfilled:
  a) the client or Juniper has provided appropriate safeguards in relation to the transfer;
  b) the data subject has enforceable rights and effective legal remedies;
  c) Juniper complies with its obligations under the data protection legislation by providing an adequate level of protection to any personal data that is transferred;
  d) Juniper complies with reasonable instructions notified to it in advance by the client with respect to the processing of the personal data;
  e) an International Data Transfer Agreement (IDTA) issued under Section 119A of the Data Protection Act 2018 is completed to comply with Article 46 of the UK GDPR.

- will assist the client, at the client's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the data protection legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

- notify the client without undue delay on becoming aware of a personal data breach; and

- at the written direction of the client, delete or return personal data and copies thereof to the client on termination of the contract unless required by applicable law to store the personal data.

The client will provide general authorisation for Juniper to engage third-party personal data processors under the contract. Juniper confirms that it will ensure these arrangements are governed by a written agreement that reflects the data protection terms set out in this policy.

Either party may, at any time on not less than 30 days' notice, revise this policy by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to the contract).

Data Processing & Sharing Agreement

Juniper and the client acknowledge that the sharing and processing of data between them may be subject to separate Data Sharing and Data Processing Agreements.

The terms and conditions of data sharing and processing, including the scope, purpose, types of data, security measures, and compliance obligations are defined in this policy.

By accepting these conditions, the client acknowledges that a separate Data Sharing and/or Data Processing Agreement may be necessary and agrees to adhere to its terms where applicable.

Juniper will retain records of processing activities which record at least the information required under Article 30(2) of the GDPR for each controller it acts on behalf of. It shall ensure that it has an appropriate agreement in place with each data controller and shall ensure that its employees, staff and contractors, receive appropriate training to enable them to ensure compliance with the instructions and contractual terms of each data controller.

Data Usage

Juniper may use anonymised client data, including pupil characteristics and assessments, for improving service quality and offerings. This usage, strictly for analysis, reporting, and supplementary services like benchmarking, will comply with the relevant data protection laws, ensuring privacy and confidentiality.

Related Procedures

This Policy should be read in conjunction with the following procedural documents, which can be found in the documents section of Juniper's HR system.

- Personal Data Breach Procedure
- Handling Data Subjects'/Information Rights Requests
- Procedure for Appointing Data Processors

Document Control and approval

Issue	Description of Change	Approval	Date of Issue
2.0	Replacement of existing policies and procedures issued in 2020 following appointment of new DPO.	CEO	18/04/2022
3.0	Replacement of Data Protection Policy to include Juniper as a data processor.	CEO	01/04/2023
4.0	Inclusion of detail around processing in the EEA; The creation of a stand alone Data Protection Policy to accompany contracts.	CFO	21/03/2024
5.0	Update of the titles of related procedural documents and addition of Appendix outlining them.	CFO	01/11/2024

Juniper

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

Junipereducation.org