All Aboard Learning Ltd

Data Protection Policy

Version: 3.0

Policy Date: 29 January 2024

Approved by: David Morgan

Next review date: 29 January 2025

All Aboard Learning Ltd
267 Banbury Road, Oxford OX2 7HT, UK
Tel: +44 1865 632965 email: support@allaboardlearning.com Co Reg: 06604357

Contents

1. Introduction and purpose

1.1 This policy sets out All Aboard Learning Ltd's (the company's) commitment to handling personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (collectively referred to as the data protection legislation).

1.2 All Aboard Learning Ltd is the data controller for the personal data it processes about customer representatives, subscribers, website users, employees, contractors, job applicants, visitors to its offices and customer leads. The company is registered with the Information Commissioner's Office (ICO) under registration number ZA090616. Details about this registration can be found at www.ico.org.uk

1.3 The purpose of this policy is to explain how the company handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on its behalf of the company's expectations in this regard.

1.4 The registered address for All Aboard Learning Ltd is 267 Banbury Road, Oxford OX2 7HT, UK.

2. Scope

2.1 This policy applies to the processing of personal data controlled by the company.

2.2 This policy also applies to the handling of our customers' personal data, where we are acting as their data processor.

2.3 This policy should be read alongside the Personal Data Breach Handling Procedure, Data Protection Request Handling Procedure and ISO 27001 processes and procedures on which training is given to all employees.

3. Definitions

3.1 There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the company. These are:

- Personal data
- Special categories of personal data
- Processing
- Data subject
- Data controller
- Data processor

3.2 These terms are explained in Appendix 1.

4. Roles and responsibilities

4.1 The Board

4.1.1 The Board has overall responsibility for ensuring the company implements this policy and continues to demonstrate compliance with the data protection legislation.

4.1.2 This policy shall be reviewed by the Board on an annual basis.

4.2 Company Director

4.2.1 David Morgan has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the company's behalf.

4.3 Data Protection Officer

4.3.1 All Aboard Learning Ltd is not required to appoint a Data Protection Officer under the data protection legislation, however it has chosen to appoint a Data Protection Officer to oversee the processing of personal data within the company, and in doing so, shall comply with Articles 37-39 of the UK GDPR.

4.3.2 The company shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office. The Data Protection Officer (DPO) can be contacted at datasecurity@allaboardlearning.com or +44 1865 632965.

4.3.3 The DPO is responsible for carrying out the following tasks:

- informing and advising the company of their obligations under the data protection legislation
- monitoring and reporting on compliance with data protection policies
- providing awareness raising and training material for employees
- carrying out data protection audits
- providing advice regarding Data Protection Impact Assessments and monitoring performance
- co-operating with the Information Commissioner's Office
- acting as the contact point for data subjects exercising their rights

4.3.4 The DPO shall report directly to the Board and shall provide updates on the company's progress and compliance with the data protection legislation.

4.3.5 All enquiries, complaints, requests and suspected breaches of security, should be referred to the Data Protection Officer and other key individuals as required.

4.4 Employees, temporary staff, contractors, visitors

4.4.1 All employees, temporary staff, contractors, visitors and other individuals processing personal data on behalf of the company, are responsible for complying with the contents of this policy. Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

4.4.2 All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the company ends. This does not affect an individual's rights in relation to whistleblowing. On termination of employment, employees shall return all information and equipment to the company, including personal identification passes/smart cards and keys.

4.4.3 Unauthorised access, use, sharing or procuring of the company's data may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

4.4.4 Employees shall have no expectation of privacy in their use of the company's systems. Any correspondence, documents, records or handwritten notes created for work related purposes, may be disclosable to data subjects under the data protection legislation, or customers under their contract.

5. Data protection by design and by default

5.1 The company is committed to ensuring that data protection considerations are at the heart of everything it does involving personal data and shall ensure that it has appropriate technical and organisational measures in place which are designed to implement the Data Protection Principles in an effective manner.

5.2 The company shall ensure that by default, it will only process personal data where it is necessary to do so, and appropriate safeguards are in place to protect it. This Data Protection Policy and supplementary policies, procedures and guides demonstrate how the company achieves their 'data protection by design and default' obligations.

6. Data Protection Principles

6.1 The data protection legislation provides a set of principles which govern how the company handles personal data. All employees, temporary staff, contractors, and other individuals processing personal data on behalf of the company are responsible for complying with the data protection principles:

6.2 Personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).

6.3 This means personal data shall only be processed where there is a lawful basis which allows this; we are fair to data subjects when we use or share their personal data (ie we must act in a way they would reasonably expect); and are transparent in how we handle personal data by describing this in our privacy notices. The company's privacy notices are available at https://allaboardlearning.com/info/policy-documents/

6.4 The data protection legislation lists the different lawful bases which permit the collection, use and sharing etc of personal data. These are contained in Article 6 of the UK GDPR. At least one of these lawful bases must apply when processing personal data. In summary:

- The data subject has given consent.
- It is necessary for contractual purposes.
- It is necessary to comply with a legal obligation.
- It is necessary to protect someone's life.
- It is necessary to carry out a task in the public interest or exercise our official duties.
- It is necessary to pursue the company's legitimate interests or a third party's legitimate interests, except where such interests are overridden by the data subject, in particular, where the data subject is a child.

6.5 When 'special categories' of personal data are processed (ie data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent.
- The processing is necessary for employment, social security or social protection purposes (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud).
- It is necessary to protect the data subject's life and they are physically or legally incapable of giving consent.
- The data subject has made the information public.
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest and are proportionate to the aim pursued.
- The processing is necessary for health or social care purposes.
- The processing is necessary for reasons of public interest in public health.

- The processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.

6.5.1 Although consent is one of the lawful bases that can be relied upon when processing personal data or special category data, it is not appropriate to rely on this for most of the processing the company does. This is because there is a high standard for achieving 'valid' consent and there are potential difficulties for the company should the data subject later withdraw their consent to the processing.

6.5.2 The company shall therefore use alternative lawful bases to legitimise its processing where they are more appropriate, such as '*processing is necessary for the performance of a contract'*, *'necessary to pursue the company's legitimate interests or a third party's legitimate interests'* and *'processing is necessary for the purposes of employment, social security or social protection purposes'.*

6.6 There are however circumstances when the company is required to obtain consent to process personal data, for example:

- To collect and use biometric information (eg fingerprints and facial images) to be used for identification purposes.
- To send direct marketing information by email or text, where the data subject would not have a reasonable expectation that their data would be used in this way or has previously objected to this.
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena (such as on social media, on the company's website; in the Press; in the company brochure; newsletter etc), where the data subject would not have a reasonable expectation that their images would be used in this way, or the rights of the data subject override the legitimate interests of the company.
- To share personal data with third parties (e.g. professionals, agencies or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

6.7 Where it is appropriate for the company to use consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent.

6.8 Consent shall not be assumed as being given if no response has been received, for example if a consent form has not been returned or a consent box ticked. The company shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing (electronic or in paper format). All forms requesting consent shall include a statement informing the person of their right to withdraw or amend their consent, and instructions on how to do this easily.

6.9 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

6.10 This means the company shall only collect and use personal data for the reasons specified or described in its privacy notices and shall not process this data in any way which could be considered incompatible with those purposes, in other words, using the data for a different or unexpected purpose.

6.11 Personal data shall be adequate, relevant and limited to what is necessary for the purpose it was processed (data minimisation).

6.12 This means the company shall ensure that any personal data collected, used or shared etc. is fit for purpose, relevant and not excessive or disproportionate for the purpose it was intended.

6.13 Personal data shall be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay (accuracy).

6.14 This means the company shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date, and where personal data is found to be inaccurate, this information shall be corrected or erased without delay.

6.14.1 The company will send annual reminders to employees to remind them to notify the company of any changes to their contact details or other information.

6.15 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed (storage limitation).

6.16 This means the company shall not keep personal data for any longer than it needs to. Personal data may be stored for longer periods where it is solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the data subject.

6.17 The company shall maintain and follow a Record Retention Schedule which sets out the timeframes for retaining and disposing of personal data. This schedule shall be available on the company's intranet.

6.18 The company shall designate responsibility for record retention and disposal to data leads, who shall adhere to the Record Retention Schedule and ensure the timely and secure disposal of the data.

6.19 Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
(integrity and confidentiality)

6.20 This means the company shall have appropriate security in place to protect personal data. The following are examples of the minimum technical and organisational measures that shall be in place to protect personal data:

6.21 Technical security measures:

- Security patches shall be applied promptly.
- Access to systems shall be restricted according to role-based requirements.
- Strong password policies shall be enforced; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others.
- Portable devices (such as laptops) and removable media (such as USBs) storing personal data shall be encrypted.
- Data shall be backed up regularly.
- The company's disaster recovery and business continuity plans shall be regularly tested to ensure data can be restored in a timely manner in the event of an incident.
- Two factor authentication (2FA) shall be enabled on systems containing sensitive data where available.
- Equipment storing personal data shall be wiped/data removed according to industry standards and best practice, prior to disposal, reuse or recycling.

6.22 Organisational security measures:

- Employees shall sign confidentiality clauses as part of their employment contract.
- Mandatory data protection awareness training shall be provided to employees during on-boarding and annually thereafter.
- Cyber security training, guidance or advice shall be cascaded to employees on a regular basis.
- Policies and guidance shall be communicated to employees on the secure handling of personal data in the office and when working remotely.
- Data protection compliance shall be a regular agenda item in Senior Management meetings. All employees shall be given the opportunity to raise compliance queries or concerns at any meeting.
- Cross cutting shredders and/or confidential waste containers shall be used to dispose of paperwork containing personal or sensitive business data.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying confidential paperwork off premises.
- Buildings and offices shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.
- Procedures shall be in place for visitors coming onto the company's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted where appropriate.
- The company shall have procedures to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

6.23 The company shall have appropriate records to demonstrate compliance with each of these data protection principles (accountability).

7. Data subjects' rights

7.1 Data subjects have several rights under the data protection legislation. The right to:

- be told how their personal data is being processed
- request access to their personal data
- request that inaccurate or incomplete personal data is rectified
- request the erasure of personal data in certain circumstances
- request the processing of their personal data is restricted in some circumstances
- request that their personal data is transferred from one organisation to another or given to them, in certain circumstances
- object to their personal data being used for public interest or direct marketing purposes
- prevent important decisions being made about them by solely automated means (including profiling)
- complain to the company about the handling of their personal data. If they remain dissatisfied with their response, they have the right to escalate this to the Information Commissioner's Office.

7.2 Data subjects may exercise their data protection rights by contacting the company in writing or verbally. Data subjects are recommended to submit their request in writing and send this to datasecurity@allaboardlearning.com or All Aboard Learning Ltd, 267 Banbury Road, Oxford OX2 7HT. The company shall handle all Data Protection Requests in line with the Data Protection Request Handling Procedure.

8. Personal data breaches

8.1 The company shall follow the Personal Data Breach Handling Procedure in the event of a personal data breach. A personal data breach is a:

'breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'.

8.2 Examples of personal data breaches include, but are not limited to:

- Emailing a group of customers and failing to insert their email addresses into the 'Bcc' field, thus revealing those email addresses to all recipients.
- Emailing or posting confidential information to the wrong person.
- Not storing or disposing of confidential paperwork securely.
- Loss or theft of IT equipment which has personal data stored on it eg a laptop, iPad, mobile phone or a USB.
- Altering, sharing or destroying personal data records without permission from the company.
- Using another person's login credentials to gain higher level access to records.
- Sharing login details or having insufficient access controls to systems, which result in unauthorised viewing, use, modification or sharing of personal data.
- Hacking into a system containing personal data.
- A social engineering incident whereby a person uses deception to manipulate individuals into divulging confidential or personal information eg a phishing email.

- A cyber-attack resulting in loss of access to personal data (eg a ransomware attack).
- Environmental incidents such as a fire or flood which damage or destroy important personal data records, prior to their scheduled disposal.
- An employee abusing their access privileges to look at someone else's records out of personal curiosity or gain.

8.3 All personal data breaches and suspected breaches (including cyber incidents) shall be reported to the Information Security Manager and Data Protection Officer immediately by emailing datasecurity@allaboardlearning.com

8.4 All incidents shall be recorded on the company security incident log and investigated by a Director (or other person as appropriate), under the support and direction of the Information Security Manager and Data Protection Officer. Cyber incidents shall be reported to and investigated by the Information Security Manager, who shall keep the Data Protection Officer informed of their findings where personal data has been compromised.

8.5 Notification to the ICO, data subjects and customers

8.5.1 The Data Protection Officer shall determine whether the company must notify the Information Commissioner's Office, data subjects or customers and will follow the Personal Data Breach Handling Procedure.

8.5.2 A personal data breach is required to be reported to the ICO within 72hrs of the company becoming aware of the breach, where the breach is likely to result in a risk to the data subject or someone else, for example if they are likely to suffer damage, discrimination, disadvantage or distress.

8.5.3 Data subjects are required to be informed without undue delay, where the breach is likely to result in 'high risks', for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm.

8.5.4 The Data Protection Officer shall notify the ICO where a personal data breach meets the 'risk' threshold. The Managing Director (or other delegated employee) shall notify data subjects following a 'high risk' breach.

8.5.5 The company has contractual obligations to notify its customers of any personal data breach (high risk or otherwise) involving their personal data. The Managing Director (or other delegated employee) shall notify customers following a personal data breach, who shall determine whether the incident is required to be notified to the Information Commissioner's Office and their data subjects.

9. Sharing data

9.1 Sharing data with other data controllers

9.2 When sharing personal data with other data controllers, for example insurance companies, brokers, accountants and solicitors, the company shall adhere to the following principles:

- Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing.

- An appropriate lawful basis shall be identified prior to the sharing.
- Data shared shall be adequate, relevant and limited to what is necessary.
- Accuracy of the data shall be checked prior to the sharing.
- Expectations regarding data retention shall be communicated.
- Data shall be shared by secure means and measures in place to protect the data when received by the third party.
- A record shall be kept of the data sharing.
- Information sharing agreements or contracts shall be in place as required.

9.3 Sharing data with suppliers (data processors)

9.4 The company uses a variety of service suppliers to help it run effectively. These are referred to as 'data processors'. This often includes companies providing services such as IT support, customer relationship management systems, data storage, communication and collaboration platforms, printing and postal services.

9.4.1 Using these data processors usually requires disclosing, storing or enabling access to personal data to them, so they can deliver the service or product the company has purchased. The data protection legislation requires that before sharing personal data with a data processor, the company must carry out due diligence checks on them to assess they have appropriate measures in place that ensures compliance with the data protection legislation and protects the rights of data subjects.

9.4.2 Due diligence checks shall be carried out on prospective data processors by the Information Security Manager, alongside the Data Protection Officer. The outcome shall be recorded on a Processor Due Diligence Report.

9.4.3 Employees shall not purchase a product or service which involves the disclosure of personal data, unless the appropriate due diligence checks have been carried out and the product has been approved by a Director (or other delegated person).

9.4.4 The company shall ensure there are appropriate Data Processing Agreements in place with its data processors which contain the relevant clauses set out in Article 28 of the UK GDPR.

9.4.5 The company shall sign Data Processing Agreements with their customers, where the company is acting as their data processor.

9.4.6 Where personal data is processed outside the UK or EEA with countries who the UK has not assessed as having 'adequate' protection for personal data, the company shall enter into UK Data Transfer Agreements with their Data Processors or customers.

10. Data Protection Impact Assessments

10.1.1 The company is required to carry out Data Protection Impact Assessment (DPIA) on the processing of personal data, where this is likely to result in 'high risks' to the rights and freedoms of data subjects. High risk means the potential for any significant physical, material or non-material harm (eg distress) to individuals.

10.1.2 A DPIA is a process which helps the company identify, minimise and document the data protection risks of a project or plan involving personal data. It demonstrates the company's compliance with the data protection principles and fulfils its 'accountability' and 'data protection by design' obligations.

10.1.3 A DPIA does not have to eradicate all risk but should minimise risks and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what the company wants to achieve.

10.1.4 The UK GDPR sets out three types of processing which will always require a DPIA:

- Systematic and extensive evaluation or profiling of individuals with significant effects
- Large scale use of sensitive data (special category or criminal conviction or offence data)
- Systematic monitoring of a publicly accessible area on a large scale

10.1.5 The company shall follow the Information Commissioner's Office supplementary list of processing, which also requires a DPIA:

- Use of innovative technology (such as Artificial Intelligence (AI))
- Denial of a service, opportunity or benefit
- Large scale profiling
- Processing of biometric or genetic data
- Data matching
- Invisible processing
- Tracking
- Targeting children or other vulnerable individuals
- Risk of physical harm

10.2 The company shall also consider the European guidelines (Guidelines on Data Protection Impact Assessment), to help identify other likely high risk processing, which includes:

- Use of sensitive data or data of a highly personal nature.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.

10.3 The company shall use their DPIA pre-screening checklist to help identify whether a DPIA should be carried out. The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA to ensure the mitigations are put in place. DPIAs shall be reviewed on an annual basis.

11. Records management

11.1 Records management is a system for managing records throughout their life cycle, from the time of creation or receipt to their destruction. The company recognises that good records management plays a crucial role in the smooth running of the company and is also necessary to comply with its obligations under the data protection legislation, particularly when responding to Subject Access Requests and protecting personal data from security threats.

11.2 The company shall manage its electronic and paper-based records in line with industry best practice.

11.3 Employees shall be provided with advice, guidance and training on how to manage the company's (and customers') records effectively throughout their lifecycle. This should include naming, storing, accessing, security classification, and disposal of records.

11.4 The company shall maintain a Record Retention Schedule and regularly review its records to ensure they are disposed of in line with the schedule. The schedule shall be communicated to data leads responsible for managing the company's and customers' records.

11.5 Record of processing activities

11.6 As a data controller, the company shall, amongst other things, know what personal data records it holds, who it shares these records with; the security in place to protect them and how long they are to be kept for. This information shall be recorded in a Record of Processing Activities Inventory (ROPA), where required, under Article 30 of the UK GDPR.

11.6.1 As a data processor, the company shall maintain a record of its processing activities in line with its processor obligations under Article 30 of the UK GDPR. This inventory shall contain the following information:

- Name and contact details of the company and its Data Protection Officer
- Description of the personal data being processed
- Categories of data subjects
- Purposes of the processing and any recipients of the data
- Information regarding any overseas data transfers and the safeguards around this
- Retention period for holding the data
- General description of the security in place to protect the data

11.6.2 This inventory shall be made available to the data controller and the Information Commissioner's Office upon request.

11.6.3 The company's ROPAs shall be reviewed annually and made available to the Information Commissioner and relevant customers upon request.

12. Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
V1.1	Update by Firebird	David Morgan	29/1/2024

Appendix 1

Data Protection Policy Definitions

Term Used	Summary Definition
Personal data	Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Special categories of personal data	Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject. It also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data relating to an individual's sex life or sexual orientation.
Processing	Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	An identifiable, living individual who is the subject of personal data.
Data controller	A data controller is an organisation who determines the purposes and means of the processing of personal data.
Data processor	A data processor is an organisation who processes personal data on behalf of a data controller, on their instruction.