Data Protection and GDPR Policy

Version Control						
Version	Author	Date	Changes	Approval	Approval Date	Review Date
1.1	L Storey-Aung	27/09/23	Policy creation	DW	28/09/23	27/09/2023
1.2	D Priestley	01/10/24	Policy review	DW	01/10/24	01/10/2025
1.3	D Priestley	01/10/25	Policy review	DW	02/10/25	01/10/2026

Data Protection and GDPR Policy

Introduction

This policy applies to all staff within Aim2Learn Ltd (A2L) meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

We must protect personal and confidential data to both comply with the law and to prove to clients, stakeholders and customers that we respect their information and/or their privacy. We are committed to all aspects of GDPR and aim to fulfil all our legal obligations, including under the GDPR regulation.

This Policy sets out how A2L commits to dealing with personal data, including personal and personal sensitive data relating to employees (i.e. personnel files) and learners.

This Policy will reflect the prevailing laws, regulations and corporate policies.

Notification

Organisations who process personal data must register with the Information Commissioner's Office (ICO), the regulator for the DPA. Our notification tells the ICO, and data subjects, about the types of information we process, giving descriptions and reasons for the processing. Our registration reference is ZA038115 (Aim2Learn Ltd).

A2L may not always be the Data Controller in relation to the processing of personal data and may be a Data Processor on behalf of another organisation. In these circumstances, A2L will process personal data in line with the wishes of the Data Controller and will at all times aim to comply with the GDPR and otherwise in line with this Policy.

Data Protection Principles under GDPR

The GDPR outlines the following principles to follow to ensure compliance with the regulation.

Personal data must be:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	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 the personal data are processed
Integrity and confidentiality	Personal data shall be 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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

These principles apply equally to personal data stored physically (for example, in paper files) and electronically.

Responsibilities

Directors	All Directors have a duty to ensure that their directorates comply with legislation affecting the handling of personal data and the supporting regulations and codes.
All Employees	All employees are accountable to their managers for compliance with this Policy and related policies, procedures, standards and guidance. All employees have a responsibility to handle personal data in accordance with the principles of the GDPR. Inappropriate processing of personal data may lead to or result in disciplinary action against individual employees.

Policy

This Policy requires the appropriate handling of Personal and Sensitive Personal Data in line with the GDPR regulations and DPA 2018. This section outlines how we will comply with the data protection Principles outlined in Section 1.

Fair, Lawful and Transparency

A2L will only process personal or sensitive personal data where specific conditions set out in the GDPR are met. Usually, the data subject's consent to process their personal data is sufficient. Explicit consent is required in order to process sensitive personal data – i.e. informed consent may not be adequate. Where consent is not held another processing condition may apply, however, a Director should be consulted in all cases to ensure compliance with the DPA 2018.

We will tell data subjects what we do with the information we hold or access about them. We will do this by including information in relevant privacy policies, fair processing notices, etc. for example, the following:

- Who the Data Controller is.
- The purpose or purposes for which the data are processed.
- Any other information to make the processing fair, e.g. include details of third parties to whom the data may be disclosed.

Specific Purpose

We will only use personal data for the purposes we have stated in our notification to the ICO and/or in line with any commitment given to a Data Controller (in our role as Data Processor) or the Data Subject directly (e.g. in line with a fair processing notice, privacy Policy, etc.).

If we have access to and use information for one purpose, we must not automatically use this information for another, potentially incompatible, purpose.

Employees who plan to use personal data for a new purpose must contact the Directors to discuss whether this processing complies with the GDPR.

Data Minimisation; Accuracy & Storage limitation

We will only collect, use and disclose the minimum amount of information needed in order to carry out any particular task or processing activity.

We will endeavour to keep records about data subjects which we hold or access accurate and up to date.

We will only keep information as long as necessary either to comply with legislation, contractual requirement, industry good practice or our own business requirements. Our Data Retention and Disposal Policy incorporates more details of data retention and secure disposal requirements.

The rights of Data Subjects

We ensure Data Subjects rights under the GDPR are protected by ensuring a data subject can request:

The right to be informed	The right to be informed encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data of individuals. The information we supply about the processing of personal data must be: • concise, transparent, intelligible and easily accessible; • written in clear and plain language, particularly if addressed to a child; and • free of charge.

The right of access	Individuals have the right to access their personal data and supplementary information. This is known as a Subject Access Request (SAR). The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

We must provide a copy of the information free of charge. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Information must be provided without delay and at the latest within one month of receipt. We will be able to extend the period of compliance by a further two months where requests are complex or numerous.

Certain data may not be disclosed where a relevant exemption applies. We will provide an explanation and a right of appeal in these circumstances.

Where we are not the Data Controller, we will forward the request to the Data Controller and otherwise assist in answering the request, where appropriate. For example, where we are a Data Processor, we will provide information we hold on behalf of the Data Controller to the Data Controller within a reasonable amount of time to allow them to respond to the request within the statutory time limits.

The right to rectification	The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete We must respond within one month. This can be extended by two months where the request for rectification is complex. If we cannot take any action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority (ICO) and to a judicial remedy. A2L employees may check their own personal information held in the HR system so that they can correct, update or delete any data. If an employee becomes aware that A2L holds any inaccurate, irrelevant or out-of-date information about them, they must update this information themselves if they are able to. If they are unable to, they must notify their line manager immediately and provide any necessary corrections or updates to the information.

The right to erasure	The right to erasure is also known as 'the right to be forgotten'. The broad principle behind this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances: ○ Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; ○ When the individual withdraws consent; ○ When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing; ○ The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR); ○ The personal data has to be erased in order to comply with a legal obligation. ○ We can refuse to comply with a request for erasure where the personal data is processed for the following reasons: ○ to exercise the right of freedom of expression and information; ○ to comply with a legal obligation for the performance of a public interest task or exercise of official authority; ○ for public health purposes in the public interest; ○ archiving purposes in the public interest, scientific research ○ historical research or statistical purposes; or the exercise or ○ defence of legal claims.
The right to restrict processing	Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data. to comply with legal or contractual obligations, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future. We will be required to restrict the processing of personal data in the following circumstances:

	• Where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data; • Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual; • When processing is unlawful, and the individual opposes erasure and requests restriction instead; • If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim; We must inform individuals when we decide to lift a restriction on processing.
The right to data portability	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability The right to data portability only applies: • to personal data an individual has provided to a controller; • where the processing is based on the individual's consent or for the performance of a contract; and • when processing is carried out by automated means We must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. We must respond without undue delay, and within one month. This can be extended by two months where the request is complex, or we receive a number of requests. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary. The information must be provided free of charge.
The right to object	If a data subject believes that the processing of personal information about them is causing, or is likely to cause, substantial and unwarranted damage or distress to them or another person, they may notify the

	organisation in writing to request A2L to put a stop to the processing of that information. Individuals have the right to object to: • processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); • direct marketing (including profiling); and • processing for purposes of scientific/ historical research and statistics. We must stop processing the personal data unless: •we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or •the processing is for the establishment, exercise or defence of legal claims. We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Rights in relation to automated decision making and profiling	The GDPR applies to all automated individual decision-making and profiling. This may be not applicable to Aim2Learn if we are not using any automated means to process personal data. Automated individual decision-making (making a decision solely by automated means without any human involvement) Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. We can only carry out this type of decision- making where the decision is: • necessary for the entry into or performance of a contract; or • authorised by Union or Member state law applicable to the controller; or • based on the individual's explicit consent.

Data Subject Access Requests should be made to david.wightman@aim2learn.org

Security of personal data

A2L must take appropriate measures to maintain the security of personal data.

Data Protection Training & Guidance

A2L employees are legally and contractually obliged to protect personal data.

A2L provides training on data protection issues to all employees who handle personal information in the course of their duties at work to help employees to understand their responsibilities as part of the statutory, compliance and continual professional development training programme.s

Transfer of personal data outside the European Economic Area

A2L will not transfer personal or sensitive personal data outside the EEA to countries other than those approved by the European Council unless personal / sensitive personal data is suitably protected.

We will only transfer and / or store personal data outside the EEA where:

- we have permission (in cases where it relates to information for which we are the Data Processor);
- we are confident it is adequately protected, i.e. we have assessed and found any risk in transferring the personal data is mitigated; and/or
- we have otherwise made the third party contractually aware of their responsibilities, for example by using EU model clauses.

Glossary of Data Protection terms

Term	Definition
Personal data	The GDPR defines what is meant by personal data. The current interpretation of personal data, taking into account legal decisions is information which: ● Identifies a living person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and ● Affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.
Sensitive personal data	Sensitive personal data are subject to stricter conditions when processing. These are details about an individual's: ● Mental or physical health; ● Racial or ethnic origin; ● Religious beliefs or other beliefs of a similar nature; ● Political opinions; ● Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); ● Sex life; ● Actual or alleged offences; ● Proceedings relating to actual or alleged offences or the sentence of any court in such proceedings. The only categories of sensitive personal data are those contained within the GDPR, as listed above. Please note that there are differences from the 'protected characteristics' outlined in the Equality Act 2010.
Data Controller	Any person (or organisation) who (either alone, jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Subject	Any living individual about whom personal data are held
Processing	Any handling of personal data. This includes (but is not limited to) collecting, recording, accessing, altering, disclosing and deleting personal data
Data Processor	Person who processes personal information on behalf of the Data Controller