AIMHIGHER LONDON LIMITED

Data Protection Policy

1. About this Policy

1.1 Aimhigher London Limited (registered office: The Granary, Brewer Street, Bletchingley, Surrey, RH1 4QP, company number: 07859881) ("Aimhigher", "the Company" "we" or "us") complies with law and regulations relating to the privacy and protection of personal data and takes these obligations seriously.

1.2 This policy sets out the principles which we apply in processing personal data of employees, customers, service-users, contacts, consultants and business partners and sets out the obligations of our staff in relation to personal data which we hold or process.

1.3 This policy applies to all of our employees and staff including both employed and self-employed staff.

1.4 This policy is prepared in compliance with the EU General Data Protection Regulation as directly effective or as otherwise implemented into UK law, as the case may be (the "GDPR").

1.5 The current Data Protection Manager is Suzanne Marchment, who may be contacted at S.Marchment@kingston.ac.uk

2. What is Personal Data

2.1 This policy relates to '**personal data**'. Personal data means any information relating to an identified or identifiable natural person ("**Data Subject**") who may be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location data, online information (e.g. an IP address) or to one or more factors relating to that person.

2.2 Sensitive Personal Data is any data which by its nature is particularly sensitive including personal data relating to or including 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 (including disability data) or data concerning a natural person's sex life or sexual orientation.

3. Data Processing Principles

3.1 Under Article 5(2) of the GDPR we are required to be able to demonstrate compliance with the data protection principles.

3.2 The data protection principles are:

3.2.1 **Lawfulness, Fairness and Transparency** Personal data must be processed lawfully, fairly and in a transparent manner.

3.2.2 **Limitation** Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3.2.3 **Minimal Processing** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Company must apply anonymisation to personal data if possible to reduce the risks to the data subjects concerned.

3.2.4 **Accuracy** Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

3.2.5 **Storage Period Limitation** Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

3.2.6 **Integrity and confidentiality** appropriate technical or organisational measures must be adopted to ensure security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

3.2.7 **Accountability** Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

4. How we ensure that data is processed fairly

Privacy Notices

4.1 Either before or at the time of collection of any personal data by us, we are required to inform data subjects about what kind of personal data we collect, the reason for collecting the data, the purposes of the processing, the legal basis which we are relying on, the data subjects rights in relation to that data, security measures taken in relation to data, whether we transfer data to third parties, the retention period and any potential transfers of data outside of the EEA.

We provide this information to data subjects in our Privacy Notice. We are required to ensure that the Privacy Notice is kept up to date. We may be required to prepare more than one Privacy Notice if we are processing different categories of data.

The Privacy Notice(s) will be reviewed by the Data Protection Manager at least annually and in any event will be reviewed if we undertake any new product or service or if we are undertaking new activities which involve the processing of personal data.

The Data Protection Manager is responsible for creating and maintaining a Register of Privacy Notices.

Authority for Processing Data

4.2 Personal data must only be processed if this is authorised by the board of directors or the Data Protection Manager and such processing is within the scope of our Privacy Notice.

4.3 If you are undertaking the processing of personal data and you do not believe it is within the scope of our Privacy Notice, please contact the Data Protection Manager]

Sensitive Personal Data

4.4 Where sensitive personal data is being collected, the Data Protection Manager must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected and the consent of the Data Subject will be required to process this data unless the Data Protection Manager agrees otherwise.

Consent

4.5 Whenever personal data processing is based on the data subject's consent Data Protection Manager is responsible for retaining a record of such consent. Data Protection Manager is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn.

4.6 Personal data must only be processed for the purpose for which they were originally collected. In the event that we wish to process personal data for another purpose, we may require the consent of the data subject concerned.

4.7 Now and in the future, Data Protection Manager must ensure that collection methods and consent statements are compliant with relevant law, good practices and industry standards.

Children

4.8 Where collection of personal data relates to a child under the age of 13, and we are relying on consent to process that data we must ensure that parental consent is given prior to the collection.

5. Data Subject Rights

5.1 Data Subjects are entitled to the following rights and we agree to honour those rights and comply with requests made by data subjects under those rights:

The right to be informed	Data subjects have a right to know about our personal data protection and data processing activities, details of which are contained in our Privacy Notices.
The right of access	Data subjects can make what is known as a Subject Access Request ("SAR") to request information about the personal data we hold about the data subject (free of charge, save for reasonable expenses for repeat requests).
The right to correction	Data subjects have a right to require that any incomplete or inaccurate information is corrected.
The right to erasure (the 'right to be forgotten')	Data subjects have a right to require that we remove data we hold about them, unless we have reasonable grounds to refuse the erasure.

The right to restrict processing	Data subjects can request that we no longer process their personal data in certain ways, whilst not requiring us to the delete the same data.
The right to data portability	Data subjects can ask us to provide copies of personal data we hold about them in a commonly used and easily storable format.
The right to object	Unless we have overriding legitimate grounds for such processing, data subjects may object to us using their personal data for direct marketing purposes (including profiling) or for research or statistical purposes.
Rights with respect to automated decision-making and profiling	Data subjects have a right not to be subject to automated decision-making (including profiling) if those decisions have a legal (or similarly significant effect) on the subject. This may not apply if the automated processing is necessary for us to perform our obligations under a contract, is permitted by law, or if explicit consent has been provided.
Right to withdraw consent	If we are relying on your consent as the basis on which we are processing a data subjects personal data, the data subject can withdraw their consent at any time. Even if a data subject has not expressly given their consent to our processing, they also have the right to object (see above).

5.2 We are required to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law.

5.3 When requests to access, correct, amend or destroy personal data records are received, the Data Protection Manager must ensure that these requests are handled within a reasonable time frame. the Data Protection Manager must also record the requests and keep a log of these.

6. Transfer of Data to Third Parties

6.1 If we are using any third-party supplier or business partner to process personal data on our behalf, Data Protection Manager is responsible for ensuring that the processor has agreed to adopt security measures to safeguard personal data that are appropriate to the associated risks.

6.2 We will also require in the contract with that supplier that:

6.2.1 the supplier provides an adequate level of data protection;

6.2.2 the supplier will only process personal data in accordance with our instructions or to carry out its obligations to us and not for any other purposes.

6.3 If we are processing personal data jointly with an independent third party, we must explicitly agree with that third party our and their respective responsibilities in the relevant contract.

7. Transfer of Data outside of the EEA

7.1 Before transferring personal data out of the UK and EEA ("European Area") we must ensure that adequate safeguards are in place which may include the signing of a relevant agreement or ensuring that an adequacy notice is in place.

7.2 Before transferring personal data outside of the European Area you must check with Data Protection Manager whether or not the relevant transfer meets relevant requirements.

8. Data Retention

8.1 In the event, for any category of document not specifically defined in this Policy and unless otherwise specified by applicable law, the required retention period for any document will be deemed to be 7 years from the date of creation of the document.

8.2 The Data Protection Manager will determine the time period for which documents and electronic records should be retained, these periods are set out in the Data Retention Schedule below.

8.3 Retention periods within Data Retention Schedule can be prolonged in the event that legal proceedings apply to the data or if there is an on-going investigation.

8.4 Any data held electronically will be subject to procedures and systems to ensure that the data is accessible during the retention period

8.5 The Company and its employees should therefore, on a regular basis, review all data which includes personal data, whether held electronically or on paper, to decide whether to destroy or delete any data once the purpose for which the documents were created is no longer relevant. The Retention Schedule sets out the default retention periods.

8.6 Once the decision is made to dispose of data, the data should be deleted, shredded or otherwise destroyed to the extent possible. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion.

8.7 Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information.

Data Retention Schedule

Document Type	**Default Retention Period**
Records relating to a contract or agreement (with a client, customer or supplier)	Seven years from end of contract or agreement

Tax records (employee and business records)	Eight years from end of the tax year to which the records relate
Records relating to employees (excluding tax, pensions and health and safety)	Three years following end of employment
Health and Safety records	Ten years
Employee pension records	Seven years from the end of employment in the case of personal pension records, eighty years from the end of your employment in the case of occupational pension records.
Marketing or business development records	Three years following last contact from subject

Please note that these are default retention periods and there may be circumstances in which the records are kept for a shorter or longer period.

9. Data Security

9.1 The need to ensure that personal data is kept securely means that precautions must be taken against loss or damage of data, accordingly both access and disclosure must be restricted.

9.2 We will take steps to ensure that there are adequate technical measures to secure personal data held by us and we will be responsible for maintaining and reviewing our technical measures. We will also take steps as an organisation to ensure that staff are aware of our and their obligations in relation to personal data generally and to take security precautions.

9.3 Employees are responsible for ensuring that they take steps to secure personal data which is under their control.

9.4 Please refer to our Data Security Policy which sets out in more detail the relevant precautions you are required to take.

9.5 All staff are responsible for ensuring that:

9.5.1 All personal data must be kept secure at all times;

9.5.2 Access to any physical location or building should be monitored and controlled;

9.5.3 Any personal data which they hold is kept, managed, transferred and destroyed in a secure manner – this includes data held electronic and in hard copy;

9.5.4 Personal information should not be disclosed to any unauthorised third party unless this is within the scope of our Privacy Notice and we have adequate safeguards in place;

9.5.5 All PCs and devices should be shut down properly when staff leave their desks for prolonged periods;

9.5.6 All devices on which personal data is stored should be password and passcode protected.

9.5.7 Passwords and passcodes should be changed regularly.

9.5.8 Memory stick usage should be minimised and all memory sticks with personal data stored on them must be password protected.

10. Data Breaches and Notification

10.1 A data breach includes but is not limited to the following:

10.1.1 Unauthorised disclosure of sensitive / personal data

10.1.2 Loss or theft of confidential or sensitive data;

10.1.3 Loss or theft of equipment on which personal data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)

10.1.4 Unauthorised use of, access to or modification of IT, data or information systems (e.g. via a hacking attack)

10.1.5 Attempts (failed or successful) to gain unauthorised access to IT, data or information systems.

10.2 If any member of staff learns of a suspected or actual personal data breach, it must be reported to the Data Protection Manager immediately. The report should include full details of the incident, when the breach occurred (dates and times), the nature of the information concerned, and how many individuals are involved.

10.3 The Data Protection Manager will perform an internal investigation and take appropriate remedial measures in a timely manner.

10.4 Where there is any risk to the rights and freedoms of data subjects, the Company must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.