

AIMHIGHER LONDON LIMITED

Privacy Notice

1. General

- 1.1 This notice is published by Aimhigher London Limited (registered office: The Granary, Brewer Street, Bletchingley, Surrey, RH1 4QP, company number: 07859881) (“Aimhigher London”, “we” or “us”). We take the privacy of your information very seriously.
- 1.2 Our Privacy Notice is designed to tell you, the user of our services about our practices regarding the collection, use and disclosure of personal information which may be provided to us directly e.g. via our website, online form, email or telephone communication or which may be provided to us by our third party partners including schools, colleges, local authorities and other organisations.
- 1.3 This notice applies to personal data processed by us as a controller. In this notice “you” refers to any individual whose personal data we hold or process (other than our staff).
- 1.4 This notice is governed by the EU General Data Protection Regulation (the “GDPR”) as directly effective or as otherwise implemented into UK law, as the case may be.
- 1.5 Please note that due to the variety of services and programmes we offer, specific privacy notices (in addition to this privacy notice) may apply to specific categories of data. If this applies to you we will supply or make available a copy of the relevant notice.

2. Personal data we collect

- 2.1 We may collect and process the following personal data (information that can be uniquely identified with you) about you:
 - 2.1.1 first name, maiden name, last name, username or similar identifier, , title, date of birth and gender, care status, information relating to your socio-economic background (including, but not limited, to pupil premiums and your eligibility for school meals), postcode, residency status, third party student reference number where a third party shares your data with us (e.g. UCAS and similar such organisations) and photographic images (“Individual Data”)
 - 2.1.2 log-in details and information you provide when setting up an account on the Site (“Login Information”);
 - 2.1.3 telephone recordings (for monitoring and training purposes) where you call us (although not all calls are recorded), recordings (including video, audio and text) from:
 - (a) any lecture, seminar, webinar, workshop or other interactive session that is recorded;
 - (b) mock exams/assessments; and

- (c) outreach
- (d) coaching sessions;
("Audio Visual Data")
- 2.1.4 postal address, email address and telephone numbers ("Contact Data")
- 2.1.6 school, year group and other current education/academic information, education/academic history, records of qualifications and/or training, personal statements and references, details of applications made to universities or other providers of tertiary education and the outcome of any such applications, including the course type and subject ("Education Data")
- 2.1.7 any information you have provided to us (or obtained through a third party such as Job Train, My First Job or LinkedIn) in your curriculum vitae, any covering letter, any application form (including name, title, address, telephone number, personal email address, date of birth, gender, employment history, qualifications and reasons for wanting to apply for the relevant position) and any information you provide to us during an workshops to help you prepare your curriculum vitae, covering letter, application or any information provided during any mock interviews ("Recruitment Data")
- 2.1.8 a record and details of any correspondence or communication between you and us or relating to any complaint submitted to us ("Communication Information");
- 2.1.9 details of your visits to our electronic services, the resources and pages that you access and any searches you make, internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform other technology on the devices you use to access the Site ("Technical Information");
- 2.1.10 replies to any surveys or questionnaires that we may use for research, evaluation and development purposes ("Survey Information");
- 2.2 We also collect, use and share data regarding school, year group, underrepresented group and other statistical or demographic data ("Aggregated Data") for any purpose. This may include, but will not be limited to:
 - 2.2.1 evaluating the effectiveness of our programmes and activities;
 - 2.2.2 monitoring how attitudes to higher education change over time; and
 - 2.2.3 targeting individuals most likely to benefit from the program.

Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity and is anonymised by us. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Notice.

- 2.3 In some circumstances we may also collect, store and use the following categories of more sensitive personal information:
- 2.3.1 information about your race or ethnicity (including first generation status);
 - 2.3.2 information about your gender identity;
 - 2.3.3 information about your sexual orientation;
 - 2.3.4 information about your religious beliefs;
 - 2.3.5 information about any disabilities or learning needs; and
 - 2.3.6 medical information;
- ("Special Category Data")
- 2.4 We will not collect any Special Category Data without your prior consent (or, if you are under 13, the consent of your parent, guardian or adult with delegated authority ("Responsible Adult")). Special Category Data is defined in the GDPR and require additional protection and consent measures. Where appropriate, we will ask for your 'explicit' consent (or, if you are under 13, the consent of a Responsible Adult) to process some of the other categories of data set out at clause 2.1 if we consider those data sets to include sensitive information.
- 2.5 Explicit consent is not a condition for accessing Aimhigher London activity unless exemptions apply (see, clause 3.1). Where these apply, they will be explained prior to the activity.
- 2.6 We will collect personal data as follows:
- 2.6.1 directly from interactions with you (including any forms or email communications we may have with you) or, if you are under 13, a Responsible Adult;
 - 2.6.2 through automated technologies or interactions (particularly with regard to Technical Data which will be collected automatically when you use our electronic services); and
 - 2.6.3 through third parties, including but not limited to:
 - (a) your school, college, university, training provider or other educational or training facilitator;
 - (b) third party education application providers such as UCAS;
 - (c) data from any tutor, seminar leader, workshop leader, external presenter or other teacher that has delivered teaching to you with us or any other education provider before;
 - (d) third party survey organisations or portal providers, such as SurveyMonkey, Google Forms and Eventbrite; and
 - (e) third party recruitment platforms such as LinkedIn.

- 2.7 If we do obtain your personal data from a third party your privacy rights under this notice are not affected and you are still able to exercise the rights contained within this notice.
- 2.8 You do not have to supply any personal information to us but you may not be able to access all our services without providing data to us (see clause 3.1 below). You may withdraw our authority to process your personal data (or request that we restrict our processing – see clause 9) at any time but we will be entitled to complete any services processing and we may need to withhold some personal data for legal or other reasons (see below).

3. Remote Sessions

- 3.1 If you access our online remote sessions, which may include online mock interviews, examinations or training or teaching or other outreach sessions delivered via video or audio conferencing services then please note that these sessions may be recorded. We may provide services to more than one individual in a group session and it may not be possible for us to remove part of the recording. As such if we do notify you that a session is being recorded and you do not wish to be recorded, please do not participate further.
- 3.2 Please note that for certain services (e.g. remote subject-specific, coaching or similar delivered sessions) a participant may be monitored through their computer or laptop via the webcam and microphone for the entirety of the session. Personal information (including Audio Visual Data) obtained through the remote sessions will be processed by us in accordance with this policy.
- 3.3 We will notify you before your participation in any recorded session. If as a participant you are aged under 13 at the time of the session, please show the provided notice to a Responsible Adult.

4. How we process your personal data

- 4.1 Personal data we hold about you will be processed either because:
- 4.1.1 the processing is necessary in pursuit of a “legitimate interest”, a legitimate interest in this context means a valid interest we have or a third party has in processing your personal data which is not overridden by your interests in data privacy and security;
 - 4.1.2 We collect your contact data for the purposes of:
 - 4.1.3 Marketing – to provide you with details of new services, invites to organised seminars, events and meetings where you have chosen to receive these. We will provide an option to unsubscribe or opt-out of further communication on any electronic marketing communication sent to you
 - 4.1.4 For research and development purposes – to better understand your needs, services and marketing requirements and develop our services and offerings
 - 4.1.5 you (or, if you are under 13, a Responsible Adult) have consented to the processing for the specific purposes described in this notice;

- 4.1.6 the processing is necessary in order for us to comply with our obligations under a contract between you and us
- 4.2 Where appropriate, we may rely on more than one legal basis to process your personal data.
- 4.3 We use legitimate interest for the purposes of marketing to collect your 'Contact data' in relation to Uni Connect signposting to establish and maintain relationships and networks of other users and service providers.
- 4.4 We use Consent for collecting your Personal data in relation to the Uni Connect Targeted Outreach and Strategic Outreach programmes to monitor your progress to evaluate the impact of our services and provide reports regarding this to our funders (the Office for Students).
- 4.5 We will generally rely on the legal basis of your consent (or, if you are under 13, the consent of a Responsible Adult) for processing Special Category Data, unless a specific exemption applies.
- 4.6 We collect and process your personal data for the following purposes:
 - 4.6.1 to register you for our programmes and services;
 - 4.6.2 to manage, maintain and amend your details with us;
 - 4.6.3 to manage our relationship with you, including:
 - (a) to notify you about changes to our terms or privacy notice;
 - (b) when you make a request for information;
 - (c) when you submit a query or complaint;
 - 4.6.4 to provide educational, academic, training and career services, resources and support including:
 - (a) lectures, seminars, webinars, workshops or other interactive sessions;
 - (b) mock exams/assessments; and
 - (c) outreach sessions;
 - 4.6.5 to establish and maintain relationships and networks of other users and service providers;
 - 4.6.6 to monitor your progress to evaluate the impact of our services and provide reports regarding this;
 - 4.6.7 to administer and protect our services, including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data;

- 4.6.8 for marketing and promotional activities through our Site, and publications and communications (including through our social media channels); and
 - 4.6.9 to use data analytics to improve the Site, services, marketing, user relationships and experiences.
- 4.7 In addition, we will collect and process Special Category Data. We collect this data for the following additional purposes:
- 4.7.1 to determine an individual's status as part of an underrepresented group; and
 - 4.7.2 to carry out equal opportunities monitoring and reporting; and
 - 4.7.3 to make anticipatory reasonable adjustments to users with disabilities for events and in person services (e.g. campus visits); and
 - 4.7.4 to provide reasonable adjustments or learning support to users; and
 - 4.7.5 to monitor and evaluate the effectiveness of a delivered activity for a particular selection of users.

5. Cookies and IP Address

- 5.1 A cookie is a piece of data stored locally on your computer and contains information about your activities on the Internet. The information in a cookie does not contain any personally identifiable information you submit to our website (the "Site").
- 5.2 On our Site, we use cookies to track users' progress, allowing us to make improvements based on usage data. We also use cookies if you log in to one of our online services to enable you to remain logged in to that service. A cookie helps you get the best out of the Site and helps us to provide you with a more customised service.
- 5.3 Once you close your browser, our access to the cookie terminates. You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. To change your browse settings you should go to your advanced preferences.
- 5.4 We are required to obtain your consent to use cookies. We will obtain this consent with a toolbar which appears when you first visit the Site.
- 5.5 If you choose not to accept the cookies, this will not affect your access to the majority of information available on our Site. However, you will not be able to make full use of our online services.
- 5.6 An Internet Protocol (IP) address is a number assigned to your computer by your Internet Service Provider (ISP), so you can access the Internet. We may use your IP address to diagnose problems with our server, report aggregate information, and determine the fastest route for your computer to use in connecting to our Site, and to administer and improve the Site.

6. Data Retention

6.1 Our current data retention policy is to delete or destroy (to the extent we are able to) the personal data we hold about you in accordance with the following:

<i>Category of personal data</i>	<i>Length of retention</i>
Personal data processed in relation to services provided by us to you	7 years from either the end of the agreement or the date you last accessed our services, being the length of time in which a party is entitled to make a legal claim
Personal data (including, but not limited to, Audio Visual Data) held in our general records	3 years from the last date on which you have interacted with us
Individual Data and Special Category Data	For the purposes of monitoring, evaluating and reporting, elements of these categories of data may be retained for up to 15 years following your graduation or until you reach 30 years of age (whichever comes first).

6.2 In some circumstances, we may keep anonymised Aggregated Data for monitoring, evaluating and reporting purposes in which case we may use this information indefinitely without further notice from you

6.3 For any category of personal data not specifically defined in this notice, and unless otherwise specified by applicable law, the required retention period for any personal data will be deemed to be 7 years from the date of receipt by us of that data or (if later) the end of the relevant contract, arrangement or interaction with that person.

6.4 The retention periods stated in this notice can be prolonged or shortened as may be required (for example, in the event that legal proceedings apply to the data or if there is an on-going investigation into the data).

6.5 We review the personal data (and the categories of personal data) we are holding on a regular basis to ensure the data we are holding is still relevant to our business and is accurate. If we discover that certain data we are holding is no longer necessary or accurate, we will take reasonable steps to correct or delete this data as may be required.

6.6 If you wish to request that data we hold about you is amended or deleted, please see clause 9 below, which explains your privacy rights.

7. **Sharing your information**

7.1 We may disclose any personal data you provide to third parties as follows (Personal data on learners who are engaged in the Uni Connect Outreach programme; aggregated data on learners who are engaged in activity through the Uni Connect Hubs programme)

7.1.1 we may host personal data with third party hosting partners such as Higher Education Access Tracker (HEAT) and the third parties who maintain the

database, London NCOP staff based at Aimhigher London and Kingston University;

- 7.1.2 where you are under 13, a Responsible Adult;
- 7.1.3 outreach Officers, employees and contractors, tutors, seminar leaders, workshop leaders, external presenters or other teachers who may facilitate or assist with the provision of our services (including GRIT, Revolution Hive);
- 7.1.4 venues, including virtual hosting platforms;
- 7.1.5 third party survey organisations and portal providers, such as Survey Monkey and Google Forms,
- 7.1.6 third party education application providers (such as UCAS), recruitment agencies, UK Higher Education Statistics Agency, government departments (including Offices for Students and Department for Education);
- 7.1.7 institutions with whom we may partner, including London NCOP, schools, colleges, universities or other providers of higher education, training or apprenticeships;
- 7.1.8 future or prospective employers;
- 7.1.9 certain third party suppliers including IT technical support providers, website developers, marketing and business development service providers may have access to personal data;
- 7.1.10 where we carry out research to gain an insight into the use of our services, the results of this research (but not your personal data itself) may be transferred to interested third parties;
- 7.1.11 if we are under a duty to disclose or share your personal data in order to comply with any legal obligation (for example, if required to do so by a court order or for the purposes of prevention of fraud or other crime);
- 7.1.12 in order to enforce any terms and conditions or agreements for our services that may apply;
- 7.1.13 our professional advisors (including lawyers, insurers and accountants);
- 7.1.14 we may transfer your personal information to a third party as part of a sale of some or all of our business and assets to any third party or as part of any business restructuring or reorganisation, but we will take steps with the aim of ensuring that your privacy rights continue to be protected;
- 7.1.15 to protect our rights, property and safety, or the rights, property and safety of our users or any other third parties. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

7.2 Other than as set out above, we shall not disclose any of your personal information unless you give us permission to do so. If we do supply your personal information to a third party we will take steps to ensure that your privacy rights are protected and that third party complies with the terms of this notice.

8. Security

8.1 We will take all reasonable steps to ensure that appropriate technical and organisational measures are carried out in order to safeguard the information we collect from you and protect against unlawful access and accidental loss or damage. These measures may include (as necessary):

8.1.1 protecting our servers by both hardware and software firewalls;

8.1.2 locating our data processing storage facilities in secure locations;

8.1.3 encrypting all data stored on our server with an industry standard encryption method that encrypts the data between your computer and our server so that in the event of your network being insecure no data is passed in a format that could easily be deciphered;

8.1.4 ensuring that all communication with our servers is encrypted through Secure Sockets Layer (SSL), an industry standard encryption method that encrypts data between your computer and our servers so that in the event of your network being insecure no data is passed in a format that could easily be deciphered;

8.1.5 when necessary, disposing of or deleting your data so it is done so securely;

8.1.6 regularly backing up and encrypting all data we hold;

8.1.7 storing paper-based data in secured cabinets; and

8.1.8 disposal of paper-based data via shredding.

8.2 Our IT networks may be hosted by a partner organisation. Where this is the case, we will review their data protection policies to ensure that it meets the standard required under GDPR.

8.3 We will ensure that our employees are aware of their privacy and data security obligations. We will take reasonable steps to ensure that the employees of third parties working on our behalf are aware of their privacy and data security obligations.

8.4 This notice and our procedures for handling personal data will be reviewed as necessary.

8.5 Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to the Site. Once we have received your information, we will use the procedures and security features referred to in this notice to try to prevent unauthorised access.

9. Your privacy rights

9.1 The GDPR gives you the following rights in respect of personal data we hold about you:

<i>The right to be informed</i>	You have a right to know about our personal data protection and data processing activities, details of which are contained in this notice.
<i>The right of access</i>	You can make what is known as a Subject Access Request (“SAR”) to request information about the personal data we hold about you (free of charge, save for reasonable expenses for repeat requests). If you wish to make a SAR please contact us as described below.
<i>The right to correction</i>	<p>Please inform us if information we hold about you is incomplete or inaccurate in any way and we will update our records as soon as possible, but in any event within one month.</p> <p>We will take reasonable steps to communicate the change to any third parties to whom we have passed the same information.</p>
<i>The right to erasure (the ‘right to be forgotten’)</i>	<p>Please notify us if you no longer wish us to hold personal data about you (although in practice it is not possible to provide our services without holding your personal data). Unless we have reasonable grounds to refuse the erasure, on receipt of such a request we will securely delete the personal data in question within one month. The data may continue to exist in certain backup, but we will take steps to ensure that it will not be accessible.</p> <p>We will communicate the erasure to any third parties to whom we have passed the same information.</p>
<i>The right to restrict processing</i>	You can request that we no longer process your personal data in certain ways, whilst not requiring us to delete the same data.
<i>The right to data portability</i>	You have right to receive copies of personal data we hold about you in a commonly used and easily storable format (please let us know a format which suits you). You may also request that we transfer your personal data directly to third party (where technically possible).
<i>The right to object</i>	Unless we have overriding legitimate grounds for such processing, you may object to us using your personal data if you feel your fundamental rights and freedoms are impacted. You may also object if we use your personal data for direct marketing purposes (including profiling) or for research or statistical purposes. Please

	notify your objection to us and we will gladly cease such processing, unless we have overriding legitimate grounds.
<i>Rights with respect to automated decision-making and profiling</i>	You have a right not to be subject to automated decision-making (including profiling) when those decisions have a legal (or similarly significant effect) on you. You are not entitled to this right when the automated processing is necessary for us to perform our obligations under a contract with you, it is permitted by law, or if you have given your explicit consent.
<i>Right to withdraw consent</i>	If we are relying on your consent as the basis on which we are processing your personal data, you have the right to withdraw your consent at any time. Even if you have not expressly given your consent to our processing, you also have the right to object (see above).

9.2 All SARs and other requests or notifications in respect of your above rights must be sent to us in writing to Suzanne Marchment at: S.Marchment@kingston.ac.uk.

9.3 We will endeavour to comply with such requests as soon as possible but in any event we will comply within one month of receipt (unless a longer period of time to respond is reasonable by virtue of the complexity or number of your requests).

10. Data Breaches

10.1 If personal data we hold about you is subject to a breach or unauthorised disclosure or access, we will report this to the Information Commissioner’s Office (ICO).

10.2 If a breach is likely to result in a risk to your data rights and freedoms, we will notify you as soon as possible.

11. Other websites

11.1 Our Site may contain links and references to other websites. Please be aware that this notice does not apply to those websites.

11.2 We cannot be responsible for the privacy policies and practices of sites that are not operated by us, even if you access them via the Site. We recommend that you check the policy of each site you visit and contact its owner or operator if you have any concerns or questions.

11.3 In addition, if you came to this Site via a third party site, we cannot be responsible for the privacy policies and practices of the owners or operators of that third party site and recommend that you check the policy of that third party site and contact its owner or operator if you have any concerns or questions.

12. Transferring your information outside Europe

- 12.1 As part of the services provided to you the information you provide to us may be transferred to, processed and stored at, countries or international organisations outside of the UK and EEA (“European Area”).
- 12.2 We may use third party organisations who are outside of the European Area and in those circumstances personal data will be transferred outside of the European Area (for instance where our services are provided online and we use third party survey organisations, portal providers or virtual meeting hosts).
- 12.3 We will not transfer the personal data of European Area users in a systematic way outside of the European Area but there may be circumstances in which certain personal information is transferred outside of the European Area, in particular:
 - 12.3.1 If you access our services while you are outside the European Area, your information may be transferred outside the European Area in order to provide you with our services;
 - 12.3.2 We may communicate with individuals or organisations outside of the European Area in providing goods and services, those communications may include personal information (such as contact information) for example you may be outside of the European Area when we communicate with you;
 - 12.3.3 From time to time your information may be stored in devices which are used by our staff outside of the European Area (but staff will be subject to our cyber-security policies).
- 12.4 If we transfer your information outside of the European Area, and the third country or international organisation in question has not been deemed by the EU Commission to have adequate data protection laws, we will provide appropriate safeguards and we will be responsible for ensuring your privacy rights continue to be protected as outlined in this notice.

13. Notification of changes to the contents of this notice

We will post details of any changes to our policy on the Site to help ensure you are always aware of the information we collect, how we use it, and in what circumstances, if any, we share it with other parties.

14. Contact us

If at any time you would like to contact us with your views about our privacy practices, or with any enquiry or complaint relating to your personal information or how it is handled, you can do so via the following email address: S.Marchment@kingston.ac.uk.

If we are unable to resolve any issues you may have or you would like to make a further complaint, you can contact the Information Commissioner’s Office by visiting <http://www.ico.org.uk/> for further assistance.