



Updated Privacy Policy (July 13, 2024)

Privacy Policy

We, at Project Access International, have a strong commitment to protect the privacy of all individuals in respect of which it processes information. We will only collect and use information in a manner consistent with your rights and our obligations under applicable law.

This Privacy Policy (the "Policy") describes how information about you is collected and used by us or shared with others, how we safeguard it and how you may access and control its use.

This Policy applies to visitors to our website located at www.projectaccess.org (the "Site") inclusive of any sub-domains of the Site, our social media pages, and to all users or potential users (mentees and mentors) of our services (the "Services").

Protecting your privacy is paramount to us. Please read the following carefully to understand our views and practices regarding your information. By using the Site and the Services and/or otherwise interacting with Project Access, you consent to us processing your personal data and other information in accordance with this Policy.

If you do not accept and agree with this Privacy Policy, you must stop using our Services immediately.

If you have any questions, concerns or comments about this Policy, please contact us at support@projectaccess.org.

Our Privacy Motto

- We are transparent about the information we hold about you.

- We will work with you to keep your information accurate and current.
- We will do our best to keep your information secure and prevent unauthorised access to it.
- We will delete information when it is no longer required to deliver our Services or when you ask us to do so and we have no legal obligation to retain such information.

Definitions

For the purpose of the General Data Protection Regulation (EU) 2016/679 (the "GDPR"), the Data Controller is Project Access. Project Access refers to the registered charity in England and Wales, Project Access International (charity number: 1190102), and our incorporated entities across the world. During the course of our charitable activities, we will process personal data about you in accordance with the GDPR.

"Personal data" means information we hold about you from which you can be or are identified. Personal data may be held in paper or electronic format or in another recorded form including photographs or video clips. It may include the following information: your name, contact details (personal and/or work details), next of kin details, criminal offences, financial background, educational background, university preferences, and expressions of opinion about you or indications of our management intentions towards you.

"Processing" means doing anything with personal data, such as accessing, disclosing, destroying, transferring, holding, amending, deleting or using the personal data.

We will comply with the six key principles in the GDPR. Your personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step 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 without delay ('accuracy');
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- 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 ('integrity and confidentiality').

Quick Guide to Content

1. Data collection
2. Cookies and analytics
3. Data processing
4. Data sharing
5. Aggregated and anonymised data
6. Data security
7. Data retention
8. Your rights
9. Consent to processing and transfer of information outside of EEA
10. Third party websites

11. Changes to our Policy

1 Data collection

We are a mentorship network for helping students apply to top universities worldwide. We continuously expand our network and our focus is on building close, long-term relationships that enable us to deliver this service free of charge to those who need it. To do our job well and connect people in the best possible way, we need to understand our Mentees and Mentors well. To achieve the above, we create detailed profiles about our Mentees and Mentors to understand exactly who they are.

We generally collect six categories of personal data:

- Personal data we collect from Mentees.
- Personal data that we collect from Mentors.
- Personal data that we collect from Content Contributors.
- Personal data that we collect from Donors.
- Personal data that we collect from Team Members.
- Personal data we get from Visitors to our Site and social media pages.

We may collect and process the following data about you:

- Information that you provide by filling in forms on the Site.
- Information that you share with us at special events that we host.
- Information that you share with us over email or social media exchanges and in questionnaires.
- Information that third parties who have worked with you or have otherwise interacted with you, share with us.

1.1 Mentees

We may collect the following personal data when potential Mentees sign up to receive our emails:

- Contact details; and

-

Our lawful basis for processing is consent.

We may collect the following personal data when Mentees sign up to our mentorship platform:

- Contact details;
- Date of birth;
- Hobbies, interests and career plans;
- LinkedIn profile link;
- Inequality data such as demographics, socioeconomic background, geography and access to information;
- Educational background such as school, predicted grades and past degrees (if applicable);
- University preferences such as university, course and topics of interest; and
- Application outcomes such as conditional offers and final acceptance.

Our lawful basis for processing is to raise and fulfil a contract.

We process special category data, specifically ethnicity, for equality of opportunity in the public interest (Article 9(2)(g), Schedule 1 of the DPA 2018).

We use automated algorithms to match Mentees and Mentors based on the personal data provided. However, any decision for matching will have the final sign-off by a Project Access team member.

1.2 Mentors

We may collect the following personal data when potential Mentors sign up to receive our emails:

- Contact details;
- Country; and
-

Our lawful basis for processing is consent.

We may collect the following personal data when Mentors sign up to our mentorship platform:

- Contact details;
- Date of birth;
- LinkedIn profile link;
- Mentoring experience;
- Inequality data such as demographics, socioeconomic background, geography and access to information;
- Educational background data such as school, offers received and past degrees (if applicable);
- University data such as university name, course, college, entry dates and graduation dates; and

Our lawful basis for processing is to raise and fulfil a contract.

We process special category data, specifically ethnicity, for equality of opportunity in the public interest (Article 9(2)(g), Schedule 1 of the DPA 2018).

We use automated algorithms to match Mentees and Mentors based on the personal data provided. However, any decision for matching will have the final sign-off by a Project Access team member.

We don't require you to provide special category data (i.e. ethnicity), but if you do provide such data, you consent to our use of it for publishing both online and in print.

1.3 Donors

We may collect the following personal data when donors make a contribution:

- Contact details;
- IP address;
- Country; and
- Donation amount.

Our lawful basis for processing is to raise and fulfill a contract. We will not contact you for the purposes of direct marketing without your explicit consent.

1.4 Team Members

We may collect the following personal data when potential Team Members sign up to receive our emails:

- Contact details;
- Country; and
-

Our lawful basis for processing is consent.

We collect the following personal data when potential Team Members send us an application for a volunteer or job opening:

- Contact details;
- Country;
- University;
- CV; and
- Responses to interview questions.

Our lawful basis for processing is legitimate interests.

We may collect the following personal data when Team Members are on-boarded:

- Contact details;
- Date of birth;
- University details;
- Contract dates and details; and
- Optional profile picture.

Our lawful basis for processing is to raise and fulfil a contract.

We process special category data, specifically ethnicity, for equality of opportunity in the public interest (Article 9(2)(g), Schedule 1 of the DPA 2018).

1.5 Visitors to our Site and social media pages

When you visit the Site, visit our social media pages or interact with the Services, we may use a variety of technologies that automatically or passively collect information about how the Site is used ("Usage data").

We collect the following data when users visit our Site: IP address and Usage data.

Usage data may include weblogs and other communication data, browser type, operating system, the page served, the duration of your visit, the time, referring URLs and other information normally transmitted in HTTP requests. Usage Data is statistical data about our users' browsing actions and patterns and does not identify any individual. We will treat Usage data as personal data if we combine it with you as a specific and identifiable person.

Our lawful basis for processing is legitimate interests.

2 Cookies and analytics

Project Access ("us", "we", or "our") uses cookies on its website (the "Service"). When you use and access our website and services, we may place a number of cookie files in your web browser. By using our services, you consent to the use of cookies.

Cookies are small pieces of text sent by your web browser by a website you visit. A cookie file is stored in your web browser and allows the Service or a third-party to recognize you and make your next visit easier and the Service more useful to you. By browsing the Site you agree to having these cookies placed on your computer. The cookies collect information in an anonymous form, including the number of visitors to a website, from where visitors to a website have come from and the pages visited.

Cookies can be "persistent" or "session" cookies. Persistent cookies remain on your personal computer or mobile device when you go offline, while session cookies are deleted as soon as you close your web browser.

We use cookies for the following purposes:

1. To enable certain functions of the Service

2. To provide analytics
3. To store your preferences

We use both session and persistent cookies on the Service and we use different types of cookies to run the Service. We may use essential cookies to authenticate users and prevent fraudulent use of user accounts. In addition to our own cookies, we may also use various third-parties cookies to report usage statistics of the Service (e.g. Google Analytics).

If you'd like to delete cookies or instruct your web browser to delete or refuse cookies, please visit the help pages of your web browser. Please note, however, that if you delete cookies or refuse to accept them, you might not be able to use all of the features we offer, you may not be able to store your preferences, and some of our pages might not display properly.

- For the Chrome web browser, please visit this page from Google: <https://support.google.com/accounts/answer/32050>
- For the Internet Explorer web browser, please visit this page from Microsoft: <http://support.microsoft.com/kb/278835>
- For the Firefox web browser, please visit this page from Mozilla: <https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored>
- For the Safari web browser, please visit this page from Apple: https://support.apple.com/kb/PH21411?locale=en_US
- For any other web browser, please visit your web browser's official web pages.

2.1 Google Services

We use Google Analytics 4, Google Tag Manager and Google Ads for performance measurement, better targeting advertisements, and marketing purposes. We collect anonymous data about the users of our sites such as how often they visit, what pages they visit, what time they visit, how long they stay and what country they are visiting from.

In compliance with EU consent policy, Consent Mode v2 was implemented on our Site. This implies that when you visit our Site, we ask for your consent to collect

data. Before you provide consent, only basic data necessary for website functionality is collected. If you provide consent, Google services collect additional data to help us understand and analyze user interactions with our Site more effectively.

You can prevent Google Analytics from collecting the above-mentioned information by installing the google opt-out browser add-on: <https://tools.google.com/dlpage/gaoptout>. However, if you block all cookies, you may not be allowed access to all or parts of our site, and some functions and features of the Site and/or the Services may not work properly.

To learn how Google uses data collected from our Site please see the following link: <https://policies.google.com/privacy/partners?hl=en-GB&gl=uk>.

3 Data processing

Your personal data has only been collected, utilised or shared by Project Access if one or more of the following applies:

- you have consented to the processing (e.g. by acknowledging your understanding of and accepting the terms of our Privacy Policy through onboarding);
- the processing is necessary for the performance of (or entering into) a contract;
- the processing is a result of an existing legal obligation to which we are subject;
- the processing is in your vital interests;
- the processing is in the public interest; or
- the processing is in our legitimate interests.

We use the information you provide to us to:

- Provide you with relevant information and services;
- Share information with mentors and the country team responsible for connecting you with that mentor;

- Ensure that content from the Site is presented in the most effective manner for you;
- Carry out our obligations arising from any contracts entered between you and us;
- Invite you and allow you to take part in special events that we host from time to time;
- Respond to communications from you;
- Ask for feedback from you to improve our Services;
- Analyse your activity on our Services to make improvements; and
- Ensure safeguarding procedures are met.

We will keep the personal data we store about you accurate and up to date. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you. We will not keep your personal data for longer than is necessary for the purpose. This means that data will be erased from our systems or anonymised when it is no longer required.

Any email marketing messages we send are done so through an EMS (email marketing service). An EMS is a third party service provider of software / applications that allows marketers to send out email marketing campaigns to a list of users. Our EMS is SendGrid. Email marketing messages that we send may contain tracked clickable links or similar server technologies in order to track subscriber activity within email marketing messages. Where used, such marketing messages may record a range of data such as; times, dates, IP addresses, opens, clicks, forwards, geographic and demographic data. Such data, within its limitations will show the activity each subscriber made for that email campaign. Any email marketing messages we send are in accordance with the GDPR and the PECR. We provide you with an easy method to withdraw your consent (unsubscribe) or manage your preferences at any time. See any marketing messages for instructions on how to unsubscribe or manage your preferences, you can also contact the EMS provider (SendGrid).

4 Data sharing

We will not share your information with any third parties for the purposes of direct marketing.

We use data processors who are third parties who provide elements of services for us. We have contracts in place with our data processors. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

In some circumstances we are legally obliged to share information. For example, when we are involved in legal proceedings such as a safeguarding incident, or when we are complying with the requirements of legislation, a court order, or a governmental or regulatory authority.

Where we share your data with a third party, we will have regard to the six data protection principles.

We may disclose your personal information to third parties:

- If Project Access or substantially all of its assets are acquired by a third party, in which case personal data held by it will be one of the transferred assets. If any of your personal data is to be transferred in such a manner, you will be contacted in advance and informed of the changes.
- If we are under a duty to disclose or share your personal data in order to comply with any legal or regulatory obligation or request.
- To enforce a contract entered into between you and us.
- To investigate potential breaches.
- To protect the rights, property or safety of our Mentees, Mentors or anyone else. This includes exchanging information with other organisations for the purposes of fraud protection, the checking of criminal records and other references.

Currently, we may share information with the following organisations, who operate under their own privacy policies referenced below.

- **Typeform L.** for the purposes of collecting information from our Mentees, Mentors and Team Members . Privacy Policy [here](#).

- **Microsoft Corporation** for the purposes of data storage and internal collaboration. Privacy Policy [here](#).
- **SendGrid, Inc.** for the purpose of managing our mailing lists. Privacy Policy [here](#).
- **Squarespace Ireland Ltd.** for the purpose of hosting our websites. Privacy Policy [here](#).
- **Donorbox (Rebel Idealist LLC)** for the purpose of managing our donor payments. Privacy Policy [here](#).
- **Stripe, Inc.** for the purpose of managing our payments. Privacy Policy [here](#).
- **Slack Technologies, Inc.** for the purposes of internal communication and collaboration. Privacy Policy [here](#).
- **UCAS Strobe** for the purpose of retrieving the impact of our services. Privacy Policy [here](#).
-

5 Aggregated and anonymised data

We may combine your Usage Data and/or your personal data with those of other users of the Services and the Site and share or provide this trend information in aggregated and anonymised form with third parties, such as prospective investors, affiliates, partners, advertisers and research bodies. This will only ever be anonymised data, and will never be capable of personally identifying an individual, and, will only be shared in accordance with applicable law. For example, we may anonymise your personal information and use it in aggregated form in order to report on industry, marketing and employment trends.

6 Data security

We will take appropriate steps to ensure that the processing of personal data is lawful or authorised, and to prevent the accidental loss, or damage to, personal data. We continuously strive, in accordance with industry standards, to have in place procedures and technologies to maintain the security of all personal data and confidential data from the point of collection to the point of destruction.

We transfer personal data to third parties where they agree to comply with similar procedures and policies or have in place adequate measures. An adequate measure would be a privacy shield certification, a Data Processing Agreement or a contract based on the EU Model Clauses.

To protect your personal data we have put in place suitable physical, electronic and managerial procedures to safeguard and secure data collected through our Services. Steps we take to secure and protect your data include:

1. Regular backups of your data including retention policies;
2. Mailbox and data access auditing;
3. Full SSL (https) connection to our Site;
4. User-level authentication to personal data;
5. Data loss prevention policies; and

Please remember that the transmission of information via the internet is not completely secure. We will do our best to protect your information, but we cannot guarantee the security of your data transmitted to our Site. Any transmission is at your own risk. Once we have received your information, we will use security features to try to prevent unauthorised and unlawful access.

If a security breach causes an unauthorised intrusion into our system that materially or non-materially provides a risk to you, we will notify you as soon as possible and later report the action we took in response to any breach.

7 Data retention

7.1 Personal Data Retention

We will not retain your personal data longer than is necessary to fulfil the purposes for which it was collected. We do this in order to comply with GDP regulations.

- **Mentors:** we collect your personal data when you sign up and, if your application is successful, when you are onboarded as a PA mentor, in order to a) be able to pair you with mentees, and b) provide you with the information

you'll require to fulfil your mentorship duties (i.e. platform updates, matching requests, and other important announcements).

- **Mentees:** we collect your personal data when you sign up and, if your application is successful, when you are onboarded as a PA mentee, in order to a) be able to pair you with mentors, and b) provide you with the information you'll require to complete your mentorship (i.e. platform updates, matching requests, and other important announcements).
- **Team members:** we collect your personal data when you apply and, if your application is successful, when you are onboarded as a PA team member, in order to a) be able to process your application, and b) facilitate you being a PA team member.

Note that the following data retention practices apply for non-active mentors, mentees, and team members:

Mentors:

Inactivity:

If a mentor is 'Inactive' (i.e. the mentoring capacity they indicate on their profile is 0) for 24 consecutive months, we will delete their profile from our pairing database and stop holding their personal data (i.e. we will anonymise any remaining data we hold).

The legal basis for this is consent. Mentors consent when they apply to become a PA mentor.

Rejected applicants:

If someone applies to become a Project Access mentor but their application is rejected, we will hold their personal data for 12 months, after which we'll anonymise their data (i.e. we will stop holding their personal data).

The legal basis for this is consent. Applicants consent when they apply to become a PA mentor.

Mentees:

Inactivity:

If it has been 24 months since a mentee has been an active participant on one of our mentorship programmes (i.e. it has been 24 months since the September in a

mentees' reported 'Target enrolment' year), we will delete their profile from our pairing database and stop holding their personal data (i.e. we will anonymise any remaining data we hold).

The legal basis for this is consent. Mentees consent when they apply to become a PA mentor.

Rejected applicants:

If someone applies to become a Project Access mentee but their application is rejected, we will hold their personal data for 12 months, after which we'll anonymise their data (i.e. we will stop holding their personal data).

The legal basis for this is consent. Applicants consent when they apply to become a PA mentee.

Team Members:

After leaving PA:

When team members are offboarded (i.e. they stop being a PA team member), we reserve the right to add them to our 'Alumni' network, providing that the team member wishes to be added. Team members who are added to our 'Alumni' network have their personal data held until they opt out of the scheme.

If team members are not added to our 'Alumni' network, or notify us that they wish to leave it after initially joining it, we will hold their personal data for 12 months, after which we'll anonymise their data (i.e. we will stop holding their personal data).

The legal basis for this is consent.

Rejected applicants:

If someone applies to become a Project Access team member but their application is rejected, we will hold their personal data for 12 months, after which we'll anonymise their data (i.e. we will stop holding their personal data).

The legal basis for this is consent. Applicants consent when they apply to become a PA team member.

7.2 Legal Obligations

However, we may be required by applicable laws and/or regulations to hold your personal data longer than this period. If no contradicting legal obligation exists, we reserve the right to anonymise mentor and mentee profiles (i.e. delete them from our database which we use to pair mentors and mentees, and remove any personal data which can be used to identify individuals) in the following situations:

Additionally, where there is a contradicting statutory obligation for us to retain your personal data, we will restrict/block further processing and then erase the relevant personal data when we no longer have a requirement to retain it.

8 Rights

You have:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

Please note that all these rights are qualified in various ways. For example, where we store your personal data for statistical purposes, we may not be able to comply with an erasure request where it would likely impair such statistical purposes or where we require your personal data for compliance with a legal obligation or in connection with legal proceedings.

You may contact our team about all issues related to this Policy, your personal data and to exercise your rights under Data Protection laws. You must make the request in writing specifying the nature of your request. All such written requests should be sent to support@projectaccess.org.

You can exercise your rights to erasure at any time by contacting us at support@projectaccess.org. We will however have to retain your name so that

we can record the fact that you do not want us to retain information about you.

If you feel that the processing of your personal data is not in line with our data protection obligations, you can complain to our lead data protection supervisory authority:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Phone: 0303 123 1113

Website: <https://ico.org.uk/>

9 Consent to processing and transfer of information outside the EEA

We are a charity registered in England and Wales that operates globally, with mentors and mentees located all over the world. Consequently, our use of your information involves international data transmission, including to countries outside the European Economic Area (EEA) where data protection laws may not be considered “adequate” by the European Commission. We will transfer your personal data to entities within Project Access. Additionally, we may transfer your personal data to third-party contractors and partners both within and outside the EEA, including the United States.

For data transfers to countries without an adequacy decision by the European Commission, we use several mechanisms to ensure the protection of your data:

1. **Standard Contractual Clauses (SCCs):** We employ the latest SCCs published by the European Commission in 2021 for new contracts and have updated existing contracts accordingly.
2. **International Data Transfer Agreement (IDTA):** For transfers from the UK, we use the IDTA or the UK Addendum to the EU SCCs, as required by the UK

GDPR.

3. **Binding Corporate Rules (BCRs):** Where applicable, we use BCRs for intra-group international data transfers.

If you are based in the European Union, please note that information we collect about you may be transferred to and processed outside of the EU. By using our Site and Services, or by providing us with any information, you consent to the collection, processing, maintenance, and transfer of such information to countries outside of the EU where there may be no local supervisory authority and where privacy rights may not be as comprehensive or equivalent to those in your country of residence.

Further Considerations:

1. **Transfer Impact Assessments (TIAs):** As per the Schrems II ruling, we conduct TIAs for transfers to countries without an adequacy decision to ensure that the data receives protection equivalent to the GDPR standards after export.
2. **Adequacy Decisions:** The European Commission has declared several countries as providing adequate protection for personal data. For transfers to these countries, additional safeguards are not required.
3. **Derogations:** In specific situations, we may rely on derogations under Article 49 of the GDPR, such as when the data subject has given explicit consent for the transfer or when the transfer is necessary for the performance of a contract.

10 Third party websites

The Site may contain links to and from the websites of our partner networks, advertisers and affiliates or other third parties and the Services may appear on third party websites and online media. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we cannot and do not accept any responsibility or liability for these policies. Please check these policies carefully before you submit any personal data to these websites.

11 Changes to our Policy

We may change this Policy from time to time, in whole or part, at our sole discretion. We encourage you to check our website to view the most recent version of this Policy. You may also request a copy of the most recent version of this Policy by contacting us. If, at any time, we decide to use your personal data for a purpose that is different from the original purpose of collecting your personal data, we may contact you regarding this change.

Last update: July 13, 2024

Remember: you can always get in touch! We really do welcome any questions, comments and requests you may have regarding this Policy. You can contact us by emailing support@projectaccess.org.