British Council China Mainland Privacy Policy (English Version)

26 January2026

British Council China Mainland Privacy Policy (English Version)

Last Updated: 26 January 2026 **Effective Date**: 13 February 2026

Summary

This Privacy Policy explains how the British Council Entities* (hereinafter referred to as "we" or "the organization") collects, uses, stores, protects, shares, and manages your personal information in accordance with relevant laws and regulations of the People's Republic of China (hereinafter referred to as "China"), including but not limited to the Personal Information Protection Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China, and the Data Security Law of the People's Republic of China. We are committed to processing your information in a transparent and compliant manner and safeguarding your rights.

Scope of Application

This policy applies to all services we provide, including but not limited to our websites, mobile applications, course registrations, examination services, event participation, consultations, and any other means by which you interact with us. When you use any individual service, this policy and any specific privacy clauses that may exist for that service (the "Specific Clauses") shall simultaneously become binding upon you. If there is any inconsistency between the Specific Clauses and this policy, the Specific Clauses shall prevail within the scope of their constraints. If this policy does not apply to a particular service, we will make this clear through appropriate means.

***Note:**

The British Council in China includes the following entities:

- **Examination Services:** BC Education Consulting (Beijing) Co., Ltd.
- **English Education**: Yinghe Advertising (Beijing) Co., Ltd.
- **Cultural Exchange**: Cultural and Education Section, British Consulate-General

This Policy Will Help You Understand the Following:

1. How we collect and use personal information
2. How we entrust processing, share, transfer, or publicly disclose your personal information
3. Retention period of your personal information
4. How your personal information is transferred across borders
5. How we protect your personal information security
6. Your rights
7. How we handle personal information of minors
8. Third-party services
9. How this policy is updated

10. How to contact us

1. How We Collect and Use Personal Information

The definitions of "personal information" and "sensitive personal information" in this policy are as follows:

"Personal information" refers to various types of information, recorded electronically or otherwise, relating to an identified or identifiable natural person, excluding information that has been anonymized.

"Sensitive personal information" refers to personal information whose leakage or illegal use may easily infringe upon a natural person's dignity or endanger their personal or property safety, including biometric data, religious beliefs, specific identities, medical and health information, financial accounts, location tracking data, and personal information of minors under the age of fourteen.

When you use British Council products and related services or interact with us, we may collect your personal information. Depending on the products or services you use and the nature of your interactions with us, the specific types of data collected may vary. If sensitive personal information is involved, we will inform you of the necessity of processing such information and its impact on personal rights as required by law and obtain your separate consent. You are not obligated to provide us with personal information; however, in certain circumstances, if you choose not to provide it, we may be unable to provide you with relevant products or services or respond to or resolve the information requests or issues you encounter.

If we need to use your personal information for purposes not specified in this policy, we will fully inform you of the purpose, method, and scope of information collection and use in accordance with legal requirements and seek your consent again. If we intend to use your personal information collected for a specific purpose for another purpose, we will also obtain your prior consent.

Scenarios in which we collect and use your personal information include:

- **Customer Service**

  When you contact us through our webforms, social media, online chat, by email, or talk to our agents/operators, we may collect personal information you provide to us. This may include: your identification data (name, contact details), professional data (workplace, position), financial/payment data; details of previous interactions with us, such as queries, etc. We may occasionally collect health related information, for example, if you need to cancel your attendance to an exam.

  We will process your information in relation to your request, such as to deal with your customer enquiry, to provide you with information about our products or activities, to manage our relationship with you or to help us improve customer experience.

  We may rely on several lawful bases when we process your data: a) your consent, if you are not a client and have a query, wish to sign up for one of our events, or to receive our newsletters; b) if you have registered for one of our courses or examinations, or wish to purchase any product from us, our lawful basis is the contractual relationship with you, or

on the pre-contractual nature of the service requested; c) when you speak to our operators, we may record calls for the purpose of conducting random quality checks that help us improve our customer assistance by phone, based on prior consents gathered by our customer assistance during the conversation to provide ongoing development to our operators and to deliver a continued quality service.

We may use AI functionality to generate summaries of any previous engagements you have had with our agents, so they can provide a personalised response, and also to generate suggested responses which the agent can review and select the most appropriate to each situation. We rely on your consents to improve the quality of our service to customers by applying this technology, while decisions and actions are always taken by our operators.

We will retain your personal information in line with our data retention schedules and with regulatory or legal requirements.

- **Marketing**

  With your consent we'll use your personal information to send you direct marketing and to better identify products and services that interest you. We do that if you're one of our customers or if you've been in touch with us another way (such as registering to attend a British Council event or entering a competition).

  This means we'll:

  - better understand you as a customer and tailor the marketing communications we send you,
  - tell you about other products and services you might be interested in,
  - try to identify products and services you're interested in.

  The information processed consists of:

  - Your contact details. This includes your name, gender, address, phone number, date of birth and email address.
  - Information from cookies and tags placed on your connected devices.
  - Information from other organisations such as aggregated demographic data and publicly available sources like the business directories.
  - Details of the products and services you've bought and how you use them.

  We'll send you information about the products and services we provide by phone, post, email, text message, online banner advertising according to the communications channels you prefer. We also use the information we have about you to personalise these messages wherever we can as we believe it is important to make them relevant to you. We do this based on your consents to receive personalized message notification. We also check that you are happy for us to send you marketing messages before we do so. In each message we send, you also have the option to opt out.

  We'll only market other organisations' products and services if you have said it is OK for us to do so.

  You can ask us to stop sending you marketing information or withdraw your permission at any time.

- **Social Media Marketing**

We may use common and compliant social media platforms for our digital marketing campaigns aimed at our customers or at new similar audiences, by using ‘list-based’ and ‘lookalike’ tools. We do this by uploading your contact data in pseudonymised format, e.g. a list of email addresses which is hashed and automatically deleted once used, to the social media platform to search for either user matches or new users with similar interests. These audiences will receive targeted ads on our products and services. We do not have the ability to identify who these users are or to access your accounts on these sites.

These activities take place under contractual arrangements, to ensure our advertising agency supplier acting on our behalf and their social media subcontractors only use the pseudonymised data for the provision of this service. Our advertising to these audiences is governed by the direct relationship between the social media platform and its users and we recommend you read their own privacy policies.

For social media advertising we rely on the consent you gave us to receive direct marketing from us. To identify and contact new audiences on social media platforms, we rely on your consents granted to social media platforms to increase the reach of our products and services.

If you wish to opt-out of seeing British Council ads on your social media account, you can do so on the site’s privacy settings, which offer options for users to control what ads they see on their profiles.

- **Fraud Checks**

  We undertake fraud checks on all customers because this is necessary for us to perform our contracted services to customers, by ensuring that the services we provide are duly paid for, and so that individuals themselves are protected from fraudulent transactions on their cards. Where we believe we may detect fraudulent activity we may block you from purchasing a product.

  Given the volumes of transactions we deal with, we use automated systems including third-party systems for fraud detection purposes which analyses each sale in order to make automated decisions as to whether or not we will accept a sale. We find this is a fairer, more accurate and more efficient way of conducting fraud checks since human checks would simply not be possible in the timeframes and given the volumes of customers that we deal with.

  The checks and decisions that are made look at various components including known industry indicators of fraud which our expert fraud detection provider makes available to us, as well as fraud patterns we have detected on our Sites. When combined, these generate an automated score indicating the likelihood of a fraudulent transaction. If our systems indicate a high score for you, then we may decline an order or even block you from our services. The specific fraud indicators are dynamic so will change depending on what types of fraud are being detected in the wider world, country and our sites at any time.

  You have certain rights in respect of this activity. Our fraud detection is in place to protect all our customers as well as the British Council. You have the right to contest any fraud decision made about you and to be given more information about why any such decision was made by exercising your rights as noted above, please contact: CNDisclosures@britishcouncil.org

2. How We Entrust Processing, Share, Transfer, or Publicly Disclose Your Personal Information

- **Entrusted Processing**

We may entrust third-party service providers to perform certain functions or services, including but not limited to the following purposes:

- Providing customer service, research, and marketing support;
- Personalizing services;
- Processing payment transactions;
- Conducting anti-fraud and other legal investigations.

Proper execution of these functions may require entrusting third-party service providers with processing the information you submit. Such service providers have limited access to your information, and their processing is restricted to the purposes and methods required by us. We confirm that we have signed strict confidentiality agreements and data processing agreements with companies or organizations entrusted with processing personal information, requiring them to process your personal information according to our requirements, personal information protection policies, and other relevant confidentiality and security measures. We also supervise the personal information processing activities of these entrusted parties.

- **Sharing**

We will not share your personal information with any company, organization, or individual. But the following circumstances are exceptions:

- Prior to obtaining your explicit authorization or consent: if business needs require external sharing of your personal information, we will inform you of the purpose of sharing, the name or identity, contact details, processing purpose, processing method, and types of personal information of the data recipient, and obtain your separate consent. Only after obtaining your explicit consent will we share your personal information with other parties.
- Sharing is necessary to fulfill agreements or legal documents you have signed with us.
- Sharing with authorized partners: we may share certain of your personal information with partners, processing your personal information only for the specific, clear, and lawful purposes stated in this Privacy Policy, sharing only the information necessary to provide the service, and agreeing with authorized partners on strict data protection measures requiring them to process personal information in accordance with this Privacy Policy and any other relevant confidentiality and security measures.
- Sharing with our affiliated offices/companies globally: within the scope of the purposes stated in this Privacy Policy, your personal information may be shared with our affiliated offices/companies globally. Before providing your personal information to our affiliated companies, we will make reasonable efforts to assess the legality, legitimacy, and necessity of the information to be shared and obtain your separate consent. We will supervise the processing activities of affiliated offices/companies and require them to take necessary measures to safeguard your personal information security. If our affiliated offices/companies wish to change the purpose of processing personal information, they will seek your authorization and consent again.
- Legal requirements or public safety**:** When we are certain that compliance with laws, regulations, legal procedures, or government requests; enforcement of service terms, investigation of potential violations; protection of the rights, property,

or safety of the organization, users, or any person; or response to public health, safety, or other emergencies is required, we may disclose information.

- **Transfer**

We will not transfer your personal information to any company, organization, or individual, except in the following circumstances:

  - Transfer with your separate consent: after obtaining your separate consent, we will transfer your personal information to other parties;
  - As our business continues to develop or change, we may undergo mergers, divisions, dissolution, liquidation, or similar procedures. If personal information is involved in such transfers, we will require the new entity holding your personal information to continue to be bound by this Privacy Policy; otherwise, we will require that entity to seek your separate authorization and consent anew.

- **Public Disclosure**

We will only publicly disclose your personal information under the following circumstances:

  - After obtaining your separate consent;
  - Legal disclosure: in cases of legal requirements, legal procedures, litigation, or mandatory requirements from government authorities, we may publicly disclose your personal information.

3. Retention Period of Your Personal Information

We will retain your personal information only for the period necessary to achieve the purposes described above and as required by laws and regulations. After the storage period expires, your relevant personal information will be securely and effectively destroyed or anonymized.

4. How Your Personal Information Is Transferred Across Borders

In principle, personal information collected and generated within the People's Republic of China will be stored within the People's Republic of China. After obtaining your authorization and consent and fulfilling legal obligations, we may provide your personal information to overseas entities. We will use contracts or other forms to ensure that your personal information is protected at a level no less than that specified in this policy.

5. How We Protect Your Personal Information Security

We strive to protect personal information from unauthorized access, use, disclosure, modification, damage, loss, or other forms of illegal processing by strengthening physical, managerial, and technical security measures.

In the event of a personal information security incident, we will actively fulfill our notification obligations, which may include informing you of: the basic situation of the security incident and its potential impact, the measures we have taken or will take, and recommendations for you to independently prevent and reduce risks. We will endeavor to notify you promptly via phone, email, policy push notifications, and, in specific circumstances, may issue announcements on public systems.

If you know or have reason to believe that your personal information has been lost, stolen, misappropriated, or otherwise compromised, or if there is any actual or suspected misuse of your personal information, please refer to the "How to Contact Us" section at the end of this policy.

6. Your Rights

Regarding your personal information, except as otherwise provided by laws and regulations, you have the following rights:

- You have the right to be informed and to make decisions regarding the processing of your personal information, and you may restrict or refuse our processing of your personal information;
- You have the right to access and copy your personal information;
- If you find your personal information to be inaccurate or incomplete, you have the right to request us to correct or supplement it;
- For personal information processing activities based on your consent, you have the right to withdraw your consent. Withdrawing your consent does not affect the validity of processing activities conducted based on your consent prior to withdrawal;
- You have the right to request that your personal information be transferred to another personal information processor designated by you;
- You have the right to request explanations and clarifications regarding relevant personal information processing rules;
- You have the right to request that we delete your personal information under specific circumstances;

If you have any objections to our personal information processing activities or this policy, you have the right to resolve them through legal channels.

You may submit your rights requests via the contact methods specified in the "How to Contact Us" section at the end of this policy. Please ensure your application includes your【name and information proving your identity (e.g., contacting us directly via your registration or application email, or providing identification documents (if the request involves high-risk information queries)】, so we can verify your identity and respond to your request. We may be unable to provide data you have no legal right to access (e.g., data involving others), and within the limits permitted by applicable laws and regulations, we may be unable to respond to your request, but we will explain the specific reasons to you.

7. How We Handle Personal Information of Minors

Although local laws and customs may define minors differently, we define all natural persons aged 11 (inclusive) to under 18 years old as minors. We do not process personal information of minors under the age of 11. Minor test-takers under the age of 18 should carefully read this policy with the accompaniment and assistance of their parents or guardians (minors under the age of 14 should carefully read the " Personal Information Protection Rules of the British Council for Children").

For cases where personal information of minors is collected with the consent of parents or other guardians, we will only use or publicly disclose such information when permitted by law, with the separate consent of parents or other guardians, or when necessary to protect the minor. If we discover that we have collected personal information of minors without prior verifiable separate consent from their parents or other guardians, we will make efforts to delete the relevant data as soon as possible.

We will handle personal information of minors in accordance with the principles of legitimacy, necessity, informed consent, clear purpose, security assurance, and lawful use, strictly complying

with the requirements of regulations such as the "Regulations on the Protection of Children's Personal Information on the Internet."

8. Third-Party Services

To better serve you, you may receive content or web links provided by third parties from us and our partners. Please note that we have no control over such third parties. You may choose whether or not to access third-party links, content, products, and services.

We cannot control the personal information protection and privacy policies of third parties, and such third parties are not bound by this Privacy Policy. Before submitting personal information to a third party, please ensure you have read and accepted their privacy policy.

9. How This Policy Is Updated

As applicable laws and regulations gradually improve and our business continues to adjust, we may amend this Privacy Policy in the future to better provide services. If our Privacy Policy is updated, we will publish the latest version here. If we make material changes to the Privacy Policy, we may also notify you through various channels, such as publishing a notice on our website or sending you a separate notification

Significant changes under this Privacy Policy include but are not limited to:

- Major changes in our service model, such as the purpose of processing personal information, the types of personal information processed, or the methods of using personal information;
- Major changes in our corporate structure or organizational framework, such as all changes caused by business adjustments, bankruptcy, or mergers and acquisitions;
- Changes in the main recipients of shared, transferred, or publicly disclosed personal information;
- Major changes in your rights regarding participation in personal information processing and the methods of exercising those rights;
- Changes in the responsible department, contact methods, or complaint channels for handling personal information security.

10. How to Contact Us

If you have any opinions, suggestions, questions about this Privacy Policy, or requests and inquiries regarding your personal information, you may contact us by sending an email to 【CNDisclosures@britishcouncil.org】.

Generally, unless otherwise specified in this Privacy Policy, we will respond to your rights requests and inquiries within 15 working days. For your reasonable requests, we will not charge fees in principle; however, for repeated, excessive, or unreasonable requests, we may charge a reasonable cost fee as appropriate. For illegal, non-compliant, unjustified, potentially groundless repetitive requests, requests requiring excessive technical means (e.g., requiring development of new systems or fundamental changes to current practices), requests posing risks to the legitimate rights and interests of others, or highly impractical requests, we may decline them.

Additionally, according to relevant laws, regulations, and regulatory requirements, we may be unable to respond to your requests in the following circumstances when required by competent state authorities or regulatory bodies, or under other agreed circumstances:

- Related to national security or defence security.

- Related to public safety, public health, or major public interests.
- Related to criminal investigation, prosecution, trial, and judgment enforcement.
- There is sufficient evidence that you have subjective malice or abuse of rights.
- Responding to your request would seriously harm your or another individual's or organization's legitimate rights and interests.
- To protect the life, property, or other major legitimate rights and interests of the personal information subject or others, but it is difficult to obtain their consent.
- Involving our or a third party's trade secrets.
- Other circumstances under laws, regulations, or regulatory requirements.