Bristol and West of England China Bureau

General Data Protection Policy

1. Purpose

The purpose of this policy is to:

- define the requirements of the General Data Protection Regulation (GDPR) as supplemented by The Data Protection Act 2018 (DPA 2018), in the context of the Bristol & West of England China Bureau (CB);
- clarify responsibilities and duties and set out the structure within which they will be discharged

2. Scope

This policy applies to all personal information processed by, or on behalf of, the CB. This includes personal information accessed or used by CB staff, as well as, for example, contractors, consultants and interns engaged in CB-led projects.

The formats in which personal data is handled can range from electronic, hard copy, and voice recording formats, to spoken forms of communication. Definitions of data for the purposes of Data Protection can be found in Section 4 of this policy.

3. Legislative Guidance

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Location data • Online identifier , such as a username

5. The data controller

The CB processes personal data relating to members, Directors, interns, visitors and others, and therefore is a data controller.

The CB is registered as a data controller and is exempt from registration with the ICO but follows their guidance in all matters.

6. Roles and responsibilities

This policy applies to **all CB Directors** and **interns**, and to external organisations or individuals working on the CB's behalf. The CB expects all those working on its behalf to adhere to this policy.

6.1 Board of Directors

The Board of Directors have the overall corporate responsibility for ensuring that the CB complies with all relevant data protection legal obligations.

The CB will ensure the Board of Directors receive sufficient information, in a timely manner, on the status of the CB's data protection management system to satisfy themselves that all legal requirements are being met. They will be notified of any incidents carrying major risk to the safety and security of relevant personal data and any action taken by the regulatory authorities, and of any subsequent action taken by the CB.

6.2 Chief Executive Officer

The CB's Chief Executive Officer has overall responsibility for data protection management within the CB and the implementation of its data protection policy. As the principal executive officer of the CB, she acts as the representative of the data controller on a day-to-day basis.The CEO is also the first point of contact for individuals whose data the CBprocesses, and for the ICO.

6.3 All students

All members should:

- Co-operate with the CB as far as is necessary to enable all data protection legal obligations and duties to be performed or complied with
- Report any suspected data protection incident to the CEO of the CB by emailing Dianne@chinabureau.co.uk

7. Data protection principles

The GDPR is based on data protection principles that the CB must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner

- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the CB aims to comply with these principles.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

The CB will only process personal data where the CB has at least one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the CB can **fulfil a contract** with the individual, or the individual has asked he CB to take specific steps before entering into a contract
- The data needs to be processed so that the CB can **comply with a legal obligation**
- The data needs to be processed for the **legitimate interests** of the CB or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear **consent**

  Whenever the CB first collects personal data directly from individuals the CB will provide them with the relevant information required by data protection law on how their data is processed through the use of the relevant privacy notice on the membership application.

8.2 Limitation, data minimisation and accuracy

The CB will only collect personal data for specified, explicit and legitimate reasons. The CB will explain these reasons to the individuals when the CB first collect their data by issuing them with the relevant privacy notice.

If the CB wants to use personal data for reasons other than those given when originally obtained, the CB will inform the individuals concerned before proceeding, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to fulfil their role.

When staff no longer need the personal data they hold, they must ensure it is deleted.

9. Sharing personal data

The CB will not normally share personal data with anyone else, but may do so where:

- The CB's suppliers or contractors need data to enable us to provide services to members. When doing this the CB will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a Data Processing Agreement with the supplier or contractor, if they're a Data Processor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the CB shares
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

10. Subject access requests and other rights of individuals

10.1 Data subject rights

Please refer to the CB's Statement of Intent: Data Subject Rights for further detailed information on the recognised rights of, and guidance for, Data Subjects which follows.

10.2 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the CB holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should be submitted in writing, either by letter or email to the Data protection office. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If any staff receive a subject access request they must immediately forward it to the Data Protection Officer (CEO).

10.3 Responding to subject access requests

When responding to requests the CB:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made

- Will ordinarily respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge

10.4 Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when the CB are collecting their data about how the CB use and process it (see section 9), individuals also have the right to:

- Withdraw their consent to the processing of data, where consent is needed to process it, at any time
- Ask the CB to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public task and legitimate interest
- Request a copy of agreements under which their personal data is transferred outside of the UK or the European Economic Area
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Receive certain information about CB's processing activities

- Request access to the personal data that CB holds

- Prevent procession that is likely to cause damage or distress to them or anyone else

Individuals should submit any request to exercise these rights to the Data Protection Officer. If staff receive such a request, they must immediately forward it to the Data Protection Officer.

The above rights apply only in certain circumstances. They are not absolute or unqualified rights. Guidance can be provided by the Data Protection Officer in each individual case.

11. Photographs and videos

As part of the CB's activities, the CB may take photographs and record images of individuals at events.

The CB will obtain consent from participants for photographs and videos to be taken for communication, marketing and promotional materials in person or online.

Whether the CB requires your consent or not, the CB will clearly explain to the subject how the photograph and/or video will be used.

Uses may include:

- Online on the CB's website, social media pages, press releases or newsletter

Consent can be refused or withdrawn at any time. If consent is withdrawn, the CB will delete the photograph or video and not distribute it further.

CB recognizes that the images of individuals captured by cameras are personal data which must be processed in accordance with data protection legislation.

12. Data security and storage of records

The CB will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Where the CB needs to share personal data with a third party, the CB will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

13. Disposal of records

Personal data that is no longer needed by the CB will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely.

14. Personal data breaches

CB have put in place procedures to deal with any suspected personal data breach and will notify the subject or any applicable regulator where it is legally required to do so.

15.1 Data breach procedure

In the unlikely event of a suspected data breach, the CB will inform all the relevant people based on guidance on personal data breaches produced by the ICO.

When appropriate, the CB will report the data breach to the ICO within 72 hours.

15. Policy monitoring

The DPO (CEO) is responsible for monitoring and reviewing this policy.
This policy shall be reviewed annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organisational developments.

Reviewed and adopted by the Board on 1 December 2021