DATA PROTECTION POLICY

BRITISH STUDY CENTRES
School of English

Aim	BSC Group Limited (including its subsidiaries British Study Centres Limited, Experience English Limited and British Study Centres Teacher Training Limited) ('the Company', 'we', 'us') is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.
The GDPR	The General Data Protection Regulation (GDPR) is part of the EU data protection reform package through which the European Commission aims to strengthen the rights of individuals in the digital age and simplify the rules for businesses in the EU. It will be will be directly applicable in all EU and EEA Member States as of 25 May 2018. The GDPR will significantly change the EU data protection regulatory landscape, setting stricter requirements, reaching more companies, and imposing potentially higher penalties. For example, companies must: ▪ Implement programmatic measures to ensure and actively demonstrate compliance ▪ Demonstrate a commitment to accountability ▪ Have in place appropriate training and governance ▪ Implement appropriate technical and organisational measures to protect the rights of individuals when designing a processing system and processing data ▪ Conduct data protection impact assessments of high risk processing activities ▪ Implement privacy by design and by default ▪ Implement data breach notification procedures As a result of Brexit the United Kingdom will no longer be part of the European Union. In order to ensure that the UK has adequate privacy laws that allow it to trade globally, the UK is in process of implementing UK equivalent legislation that will largely follow the GDPR, but also includes additional requirements relating to surveillance and law enforcement. We have taken this into account as part of our planning for the new legal requirements. It is the responsibility of each person within our Company to ensure that we comply with these requirements, and will be overseen by the Data Protection Officer (DPO).
Purpose	This policy sets out how we seek to protect personal data and special categories of personal data (see the 'definitions' section of this policy) so as to ensure that our staff understand the rules governing their use of such data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the DPO be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.
Scope	This policy applies to all employees, workers, volunteers, interns and contractors who must make themselves familiar with this policy and comply with its terms. For these reasons, it is important that all staff familiarise themselves with this policy, and attend all training sessions in respect of the care and handling of Personal Data. This policy does not form part of any employee's contract of employment.
Amendments to this policy	This policy supplements our other policies relating to internet and email use. The Company reserves the right to supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Review date	January 2019
Owner	Our appointed DPO has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary. DPO contact details: Angela Mynott angela.mynott@british-study.com 01273 007147

CONTENTS

1. CATEGORIES OF DATA & DEFINITIONS

BSC Group Limited is a data Controller and we hold personal data and special categories of personal data, about our employees, workers, volunteers, interns, contractors, clients, homestays, customers, suppliers and individuals for a variety of business purposes.

In order to fully appreciate the requirements of the data protection legislation it is important for you to understand the meaning of certain key words and phrases, which are used within the data protection legislation. These are set out as follows:

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: ▪ Compliance with our legal, regulatory and corporate governance obligations and good practice ▪ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests ▪ Ensuring business policies are adhered to (such as policies covering email and internet use) ▪ Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking ▪ Investigating complaints ▪ Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments ▪ Monitoring staff conduct, disciplinary matters ▪ Marketing our business ▪ Improving services
Personal data	'Personal Data' means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV's.
Special categories of personal data	'Special Categories of Personal Data' include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
Controller	'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (the 'what', 'how' and 'why'); where the purposes and means of such processing are determined by law.
Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. For example if we outsource our IT, Payroll or Occupational Health, the suppliers would be our Processors.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such

	as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for the Company is the UK Information Commissioners Office (ICO).

2. THE PRINCIPLES

The data protection legislation sets out a framework of principles, which must be followed in relation to all processing of Personal Data ('the Principles'). The Company shall comply with the Principles of and we will make every effort possible in everything we do to comply with these Principles. The Principles are:

- **First: Lawful, fair and transparent.** Personal data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
- **Second: Limited for its purpose.** Personal data can only be collected for a specific purpose.
- **Third: Data minimisation.** Any personal data collected must be necessary and not excessive for its purpose.
- **Fourth: Accurate.** The personal data we hold must be accurate and kept up to date.
- **Fifth: Retention.** We should not store personal data longer than necessary.
- **Sixth: Integrity and confidentiality.** The personal data we hold must be kept safe and secure.
- **Seventh: Accountability and transparency**

We must ensure accountability and transparency whenever we process personal data and must be able to demonstrate, how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting data protection impact assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an on-going basis

3. OUR PROCEDURES

3.1 FAIR AND LAWFUL PROCESSING

The Company must process personal data fairly and lawfully in accordance with individuals' rights under the First Principle (see section 2 above). This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If the Company cannot apply a lawful basis (explained below), our processing does not conform to the First Principle and will be unlawful. Data Subjects have the right to have any data unlawfully processed erased.

We must maintain our appropriate registration with the ICO in order to continue lawfully processing data. We hold a current registration under number Z6650403, which is accessible via the ICOs publically accessible register of data controllers. We must also maintain an electronic record of processing activities under the Company's control. These records may be made available to a Supervisory Authority/the ICO on request. The DPO is responsible for the maintenance of these records.

3.2 CONTROLLING VS PROCESSING DATA

The Company is classified as both a data Controller and a (see Definitions in section 1 above).

As a data Processor, we must comply with our contractual obligations and act only on the documented instructions of the data Controller. As a data Processor, we must:

- Not use a sub-processor without written authorisation of the data Controller
- Co-operate fully with ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the data Controller of any personal data breaches

If you are in any doubt about how we handle data, contact the DPO for clarification.

3.3 LAWFUL BASIS FOR PROCESSING DATA

The Company must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the DPO. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

- **Consent.** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

- **Contract**. The processing is necessary to fulfil or prepare a contract for the individual.

- **Legal obligation.** We have a legal obligation to process the data (excluding a contract).

- **Vital interests.** Processing the data is necessary to protect a person's life or in a medical situation.

- **Public function.** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

- **Legitimate interest.** The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

3.4 DECIDING WHICH CONDITION TO RELY ON

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonable achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Always consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

The Company's commitment to the First Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a Privacy Notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

4. SPECIAL CATEGORIES OF PERSONAL DATA

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease. If you are processing such data, please contact the DPO who will assist with establishing that we have lawful grounds for processing such data.

5. CHILDREN AND YOUNG PERSONS

Children merit particular protection when we are collecting and processing their personal data because they may be less aware of the risks involved. If we process children's personal data then we should think about the need to protect them from the outset, and design our systems and processes with this in mind. Compliance with the data protection principles and in particular fairness should be central to all our processing of children's personal data. We must have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.

If we are relying on consent as our lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. For children under this age we will need to get consent from whoever holds parental responsibility for the child - unless the online service we offer is a preventive or counselling service.

We should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them. We should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

6. RESPONSIBILITIES

The Company takes our duty to protect the data we collect seriously. In order to comply with our duties of being a Controller we will ensure that we put in place the following:

- adequate business compliance processes and procedures
- provide staff awareness training
- implement technical and organisational data security measures
- ensure that the organisation has an appropriate legal basis for its data processing activities

The Company has appointed the DPO who can be contacted for further guidance on this policy, related policies and procedures.

6.1 OUR RESPONSIBILITIES

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

6.2 YOUR RESPONSIBILITIES

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times

- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

6.3 RESPONSIBILITIES OF THE DATA PROTECTION OFFICER

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- To monitor internal compliance with the GDPR and other data protection laws, including policies and procedures on a regular basis
- To ensure staff and others are suitable trained and promote awareness on data protection
- To conduct data audits when required
- Inform and advise on data protection obligations
- Provide advice regarding Data Protection Impact Assessments (DPIAs)
- Act as a contact point for data subjects and the supervisory authority (namely, the ICO)
- To highlight and pay due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing data

6.4 RESPONSIBILITIES OF THE HEAD OF IT

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Review the related IT policies alongside the DPO to ensure compliance
- Ensuring immediate action when assisting with any reports of beach relating to a system, service, software or equipment

6.5 RESPONSIBILITIES OF THE HEAD OF MARKETING

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and this policy as well as any additional recommendations that the DPO may require

7. ACCURACY AND RELEVANCE

The Company will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Personal Data and/or Special Categories of Personal Data will be inaccurate if they are incorrect or misleading as to any matter of fact (e.g. an incorrect name or address). If you are inputting data onto our system and are unsure as to the accuracy of certain information (e.g. because you cannot read the handwriting or because it looks like an obvious mistake or omission), you should try to get in touch with the

data subject to clarify the issue. We will not be in breach of this principle, even if we are holding inaccurate personal data if:

- we accurately recorded those data when we received them from the data subject or a third party and
- we took reasonable steps to ensure the accuracy of those personal data and
- if the data subject has notified us that the personal data are inaccurate, we have taken steps to indicate this fact (e.g. by making a note that we have received an objection).

We must take reasonable steps to keep personal data up to date to the extent necessary. The purpose for which personal data are held will determine whether they need to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated. We shall check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We shall take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8. DATA SECURITY

The data protection legislation requires us to take appropriate technical and organisational measures to protect personal data and/or special categories of personal data, which we process:

- technical measures include: software controls to restrict user access; up-to-date virus checking software; audit trail software; and encryption—all of which we have in place and manage through our IT department;
- organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; and training Staff on the care and handling of data—all of which you are responsible for complying with and applying to your daily routine.

We have in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. You must keep personal data secure against loss or misuse, please also refer to the relevant IT Policies in relation to data protection. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

9. STORING DATA SECURELY

The below list is not comprehensive but aims to provide guidance to correctly storing data. At our premises, we aim to have clear desks, which means that at the end of each day and when we are not at our work area, we will not leave data available to be accessed. For example, notebooks will be locked away and computers will be locked.

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly and not easily accessible to find
- The DPO must approve any cloud used to store data following consultation with the Head of IT
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- In normal circumstances data should never be saved directly to any mobile devices such as laptops, tablets or smartphones, this includes syncing with OneDrive, Dropbox and SharePoint etc. In exceptional circumstances where data needs to be saved to a mobile device it must be encrypted with a strong encryption.
- All servers containing sensitive data must be approved and protected by security software and hardware
- All reasonable technical, electronic and physical measures must be put in place to keep data secure

10. DATA RETENTION AND MINIMISATION

We must retain personal data for no longer than is necessary (the Principle of minimisation). What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our Archiving and Minimisation Policy. All employees are responsible for ensuring that information is not kept for longer than necessary. The overriding principle is that we should minimise the data we hold wherever possible, unless we have a lawful reason to retain it. You should review the Personal Data, which you hold on a regular basis and delete any data, which are no longer required in connection with the purpose for which they were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data. You should therefore consider the type of relationship which our Group has with the data subject and whether there is an expectation that we will retain data for any given period of time (e.g. our employees would expect us to retain their data for a period of time after they had left so we could provide them with a reference, or in the event of an employment claim).

11. TRANSFERRING DATA INTERNATIONALLY

There are restrictions on international transfers of personal data. You must not transfer any Personal Data to any country or territory outside the European Economic Area (EEA), unless you are authorised to do so. The EEA comprises the EU Member States plus Iceland, Norway and Liechtenstein.

Be aware that transfers may take place that are not obvious—e.g. if a data Processor that we have appointed in the UK subcontracts some of its processing obligations to a sub-processor in India there will be a transfer of data out of the EEA (from the data Processor to the sub-processor) which will be prohibited unless certain conditions are met.

You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

12. RIGHTS OF INDIVIDUALS

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

12.1 RIGHT TO BE INFORMED

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children or when English is not the data subject's first language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

12.2 RIGHT OF ACCESS

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

Please read Section 14 of this policy for further information with regards to subject access request handling.

12.3 RIGHT TO RECTIFICATION

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

12.4 RIGHT TO ERASURE

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

Please read Section 15 of this policy for further information with regards to erasure requests.

12.5 RIGHT TO RESTRICT PROCESSING

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further.
- We must retain enough data to ensure the right to restriction is respected in the future.

Please read Section 15.3 of this policy for further information with regards to individuals' requests to restrict processing.

12.6 RIGHT TO DATA PORTABILITY

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

Please read Section 15.3 of this policy for further information with regards to portability requests.

12.7 RIGHT TO OBJECT

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Please read Section 15.3 of this policy for further information with regards to individuals' objections.

12.8 RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

13. PRIVACY NOTICES

13.1 WHEN TO SUPPLY A PRIVACY NOTICE

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

If we intend to further process the Personal Data and/or Special Categories of Personal Data for a purpose other than that for which the Personal Data was collected, we shall provide the Data Subject prior to that further processing with information. For such new activities please contact DPO prior to undertaking such activities, as we will need to assess the lawful basis of such processing.

DATA FROM OTHER SOURCES

If we receive Personal Data and/or Special Categories of Personal Data about a Data Subject from other sources, we must provide the Data Subject with the information above, together with details of the categories of Personal Data concerned and the source of the Personal Data (and, if applicable, whether it came from a public source), as soon as possible thereafter. We must inform Data Subjects whose Personal Data we process that we are the Controller with regard to that data, and we shall provide our contact details.

13.2 WHAT TO INCLUDE IN A PRIVACY NOTICE

Privacy Notices must be concise, transparent, intelligible and easily accessible.

The following information must be included in a Privacy Notice to all data subjects:

- Identification and contact information of the Controller and the DPO
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the Controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure

POSITION AND FORMAT OF DATA PROTECTION NOTICE

- The data protection notice must be reasonably prominent and in reasonably legible font
- The data protection notice must be included at every point where we collect Personal Data, such as application forms, websites, etc.

- If, for example, the data protection notice is provided online, it must be positioned so that it can be seen and not hidden behind a hypertext link and should be included in the online journey just before a ‘submit’ button.

14. SUBJECT ACCESS REQUESTS

14.1 WHAT IS A SUBJECT ACCESS REQUEST?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

14.2 HOW THE COMPANY DEALS WITH SUBJECT ACCESS REQUESTS

We must provide an individual with a copy of the information requested free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

14.3 DATA PORTABILITY REQUESTS

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the Controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one calendar month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

14.4 PROCESS

If an individual wishes to make a Subject Access Request the request should be made in writing to the DPO with the subject clearly stating ‘Subject Access Request’. If an individual struggles and finds it unreasonably difficult to make the request in writing then the Company will accept a verbal request in this scenario. Please also state if you require the response in another format such as Braille, large print, email or audio.

The Company may, when necessary, request information or evidence to verify the requestors identity, or request further detail about the data in order to locate the information which has been requested.

If the request is being made via a third party, the Company will require the written authority of the data subject to proceed with the request. Or if the request is being made on behalf of a child (under the age of 18)

then a consideration will be made as to whether the child understands their rights before the information is shared, and we may seek to gain parental or a guardian's consent.

The Company will provide a copy of the information, the source of the data, description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
An individual can also request information about the reasoning behind any automated decisions (except where this information is a trade secret).

15. RIGHT TO ERASURE

15.1 WHAT IS THE RIGHT TO ERASURE?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

15.2 HOW WE DEAL WITH THE RIGHT TO ERASURE

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

15.3 THE RIGHT TO OBJECT

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the Privacy Notice. We must offer a way for individuals to object online.

15.4 THE RIGHT TO RESTRICT AUTOMATED PROFILING OR DECISION MAKING

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

16. MARKETING

Where we undertake direct marketing activity we must comply with the General Data Protection Regulation 2018 and the Privacy and Electronic Communications Regulations 2003 (to be replaced by the forthcoming E-Privacy Regulations, when in force) which impose additional requirements to ensure that consent is freely given, specific and informed. In practice, this means that we must have explicit consent for the processing of customer data for the purposes of direct marketing. We have to bring this right explicitly to the attention of the Data Subject and presented clearly and separately from any other information. It must be clear and set out separately where we are seeking consent to market our own services and that of third parties, as well as the mediums though which we wish to market e.g. SMS, Phone, e-mail etc.

We must also the Data Subject should have the right to object to such processing (e.g. though clear and obvious unsubscribe options), including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge.

17. THIRD PARTIES

17.1 USING THIRD PARTY CONTROLLERS AND PROCESSORS

As a Controller and a Processor, the Company must have written contracts in place with any third-party Controllers and/or Processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a Controller, we must only appoint Processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a Processor, we must only act on the documented instructions of a Controller. We acknowledge our responsibilities as a data Processor under GDPR and we will protect and respect the rights of data subjects.

17.2 CONTRACTS

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with Controllers and/or Processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions

- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

If you are involved with for the selection, appointment or use of Processors, you must ensure that you only select those Processors that are able to provide us with sufficient guarantees in respect of the technical and organisational measures they will apply to the processing of Personal Data. Furthermore, if you are responsible for the drafting or negotiation of contracts with data Processors, you must ensure those contracts contain all applicable data protection provisions and first consult the DPO prior to entering into any such relationship.

18. CRIMINAL DATA

All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. As part of our recruitment process and due to our accreditation by regulatory bodies we must conduct criminal record checks for workers that meet the definition of regulated activity for working with children. Recruiting managers will be trained on dealing with disclosures, and ex-offenders will not be discriminated against. The Company is required to hold a Single Central Record (SCR) for each site, which will hold limited information on criminal checks. Access to the SCR is password protected by restricted personnel. For more details on our criminal checks please see our Recruitment Policy.

19. PUBLISHING EXAM RESULTS

The Company will not publish any exam results or share this information unnecessarily. Any results from tests our students conduct with us will be kept confidential and students will be informed of their results on an individual basis. The results from online tests via our website or other IT system, will be directly emailed to the individual and only be accessed by a secure login and password.

20. CCTV

We have CCTV in some of their schools for security and safeguarding. Where we make use of CCTV, we display clear notifications to inform visitors, students and staff when they may be captured on CCTV throughout our premises. Footage is accessible by restricted personal such as our School Directors, HR and Safeguarding Leads. We may need to share footage for investigation or disciplinary action, but also share footage with third parties such as the police to aid their investigations.

21. TAKING PHOTOGRAPHS

We recognise that photographs are taken for personal and business reasons and the ability to take photographs via a mobile device has become quick and simple. At British Study Centres we may take photographs of our students and staff for numerous business reasons including; graduation pictures, passes and to remember social activities.

We ask, or seek consent from a parent or guardian, before taking a photograph of a child under 13 years old for business use. We ensure that the photo is taken on a business device and not a personal one, and

ensure that we have consent before sharing the photograph on our website, newsletter or other promotional public facing material and social media sites.

We take care to ensure that no individual is named, when displaying photographs externally to public sites. Should an individual chose to identify themselves in a photograph via a public site, where possible, the business will review the request to identify the individual and only approve the change if we can do this.

Any request made to delete or remove a photograph will be actioned as soon as possible.

22. CREDIT CHECKS

We may feel it necessary as part of a pre-employment check to conduct a credit check for your role. Roles which may include this type of check are; roles working in Finance or Payroll and which have significant access to staff bank details, and roles which are given significant financial authority on behalf of the business and provided with a company credit card. When we conduct this type of check we will receive a report to tell us how you are managing your credit in order to make a hiring decision. For more details on our credit checks please see our Recruitment Policy.

23. AUDITS, MONITORING AND TRAINING

23.1 DATA AUDITS

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

23.2 MONITORING

Everyone must observe this policy. The DPO has overall responsibility for this policy. The Company will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

23.3 TRAINING

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

24. ASSESSING THE IMPACT OF OUR PROCESSING ACTIVITIES

In order to enhance compliance where processing operations are likely to result in a high risk, we are responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of Personal Data complies with the law. Where necessary, we shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

25. REPORTING BREACHES

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. The Company has a legal obligation to report any data breaches to the DPO within 72 hours.

All staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the DPO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures, will be liable to disciplinary action.

NOTIFYING THE INFORMATION COMMISSIONERS OFFICE (ICO)

Where applicable, the DPO will notify the ICO that we process personal data in an automated form. 'Personal data' means data that relates to a living person who can be identified from that data. It includes employment details, client information and information captured on CCTV. https://ico.org.uk/

For more information on Breaches and our breach procedure please refer to the Data Breach Management Policy.

26. FAILURE TO COMPLY

We take compliance with this policy very seriously. Failure to comply puts both you and the Company at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our Disciplinary Policy and Procedure, and serious or intentional failure to comply may be considered as gross misconduct and result in summary dismissal.

Should the Company experience reputational loss as consequence of any negative publicity, particularly if a complaint is made to the ICO or an individual makes a claim for compensation against the organisation. We will thoroughly investigate any complaint made whether or not the complaint is internal or external. If the cause of the complaint is directly or indirectly related to an action caused by a member of staff we may take disciplinary action. If the cause of the complaint is directly or indirectly related to an action caused by a worker on behalf of the business or via a Third Party, the action taken will be stipulated in the current contract.

In certain circumstances, a negligent or deliberate breach of the data protection legislation could result in personal criminal liability not just for the Company but also for our employees and other members of staff.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.