PRIVACY POLICY

These guidelines are designed to provide you with a clear understanding of our practices regarding the collection, use, and management of your personal data. We explain the reasons behind our data collection, how we use this information, and the measures we take to protect your privacy. Additionally, this document outlines the choices available to you regarding the use of your data, including how you can access, update, or control the personal information we hold about you. This ensures transparency and empowers you to make informed decisions about your personal information.

Principles of GDPR Compliance

At PLUS, we are dedicated to upholding the highest standards of data privacy and strive to handle personal data in compliance with the General Data Protection Regulation (GDPR). The following principles guide all our data processing activities.

Lawfulness, Fairness, and Transparency

PLUS ensures that all personal data processing activities are carried out lawfully, fairly, and in a transparent manner. Individuals are provided with clear and concise information about how their personal data is collected, used, and stored.

Purpose Limitation

Personal data is collected for specified, explicit, and legitimate purposes. PLUS ensures that personal data is not processed in a manner that is incompatible with these purposes.

Data Minimisation

PLUS only collects and processes personal data that is necessary and relevant for the specified purposes. Personal data is kept to a minimum and is not retained for longer than required.

Accuracy

PLUS takes reasonable steps to ensure that personal data is accurate, up to date, and kept in a reliable and secure manner. Staff members are encouraged to promptly notify the designated data protection officer of any inaccuracies or changes to personal data.

Storage Limitation

Personal data is stored for no longer than necessary for the purposes for which it was collected. Regular reviews are conducted to ensure that personal data is securely disposed of when it is no longer needed.

Security and Confidentiality

PLUS maintains appropriate technical and organisational measures to protect personal data against unauthorised access, disclosure, alteration, and destruction. Staff members are

trained on data protection practices and are obligated to maintain the confidentiality and security of personal data.

Data Subject Rights

PLUS respects the rights of individuals regarding their personal data, including the right to access, rectify, restrict processing, and erase personal data when applicable. Requests related to data subject rights are addressed promptly and in accordance with applicable data protection laws.

What Is Personal Data?

Personal data encompasses any information that can be used to identify you as a distinct individual. This type of data includes but is not limited to, your contact details such as name, address, and email; demographic information like date of birth and postcode; as well as data regarding your personal preferences and interests which help us to understand your needs and provide better service.

Sensitive Personal Data

In addition to the general personal data mentioned above, there exists a category known as sensitive personal data. This subset includes details that are more intimate in nature, such as your physical and mental health records, genetic or biometric data, political affiliations, religious or philosophical beliefs, union memberships, and sexual orientation. Information pertaining to the commission or potential commission of any offenses or related legal proceedings also falls under this category.

Given the sensitive nature of this data, our policy is to only request such information when it is absolutely essential, for example for specific applications or compliance with legal requirements. In such cases, robust protective measures are implemented to ensure the security and confidentiality of your sensitive personal data.

How We Collect Your Personal Data

At PLUS, we are committed to transparency in how we gather and use your information. This section outlines the various methods through which we collect your personal data, ensuring you understand our processes and the care we take with your information.

Direct Interactions

You may provide us with your personal data when you:

- Fill out application forms or registration documents for our programmes, either online or in hard copy.
- Communicate with us directly via phone, email, or in person to make enquiries or provide feedback.
- Subscribe to our newsletters or other communication services.

- Participate in our surveys, competitions, or promotional events.

Indirect Collection from Third Parties
Occasionally, we may receive personal data about you from third parties, which could include:

- Educational consultants and travel agents who assist in arranging your travel and enrolment in our programmes.
- Partner universities and colleges that host our summer and mini-stay programmes.
- Service providers who assist with our marketing and communication strategies.
- Recruitment agencies who assist us in recruiting staff.

Automated Technologies and Interactions
As you interact with our website, we may automatically collect technical data about your equipment, browsing actions, and patterns. This personal data may be collected by using cookies, server logs, and other similar technologies.

Public Sources and Third-Party Integrations
We might also obtain personal data about you from public sources such as educational websites, publicly accessible databases, or social media platforms, where you have chosen to make your information public. Additionally, we use third-party services that integrate with our systems to enhance our service offerings, which may involve access to your data from these providers.

Why We Collect Your Personal Data

Operational Uses

- To register and manage your participation in our programmes, ensuring that all arrangements, from accommodation to educational services, are appropriately handled.
- To process payments for our services and ensure financial transactions are accurately completed.

Communication

- To keep you informed about updates to our programmes, services, and upcoming events that might interest you.
- To respond to your inquiries and provide customer support when needed.

Legal and Regulatory Compliance

- To comply with applicable laws and regulations, including but not limited to educational standards, safeguarding requirements, and immigration laws.

- To meet our obligations under health and safety laws, and for the prevention and detection of crime or fraud.

Improvement of Services

- To analyse feedback and interactions to improve our educational and leisure programmes.
- To conduct research and analysis to develop more tailored and effective educational products.

Marketing

- To send you promotional material and communications regarding our programmes and services that we believe may be of interest to you, in accordance with your communication preferences.

Security

- To ensure the security of our online services and safeguard the information technology systems used to store and manage your personal data.

How We Protect Your Personal Data

At PLUS, we take the security of your personal data seriously and have implemented robust measures to ensure it is stored securely and confidentially and protected from unauthorised access, alteration, disclosure, or destruction. Here's how we safeguard your information:

Security Measures

- We use industry-standard security technologies to protect your personal data.
- Access to your personal data is restricted to only those employees, agents, and contractors who need to know that information in order to process it on our behalf, and they are subject to strict contractual confidentiality obligations.

Data Retention

- We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.
- After this period, your personal data will be securely deleted or anonymised so it can no longer be linked back to you.

Access Controls

- Records are stored within our password-protected system, accessible only to authorised personnel.

- We regularly review our information collection, storage, and processing practices, including physical security measures, to guard against unauthorised access to systems.
- Where we have given you (or where you have chosen) a password that enables you to access certain parts of our services, you are responsible for keeping this password confidential.

Data Breach Procedures

- In the unlikely event of a data breach, we have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Accreditation

At PLUS, we maintain a high standard of excellence in our English Language Courses, proudly accredited by the BAC and the British Council for the teaching of English in the UK. Our accreditation underscores our commitment to providing quality education and adhering to best practices in language instruction and student services.

As a necessary part of maintaining our accredited status, we undergo regular inspections conducted by the British Council and BAC. These inspections ensure that our educational programmes meet strict criteria for quality and effectiveness. During these inspections, it may be necessary to provide access to certain documents that contain personal data of our staff or homestay providers. This is essential for verifying our compliance with relevant standards and regulations.

We take the privacy and security of personal data very seriously. To safeguard this information during the inspection process, we take the following precautions:

- **Controlled Access:** Inspectors are granted access only to the information that is absolutely necessary for the purposes of the accreditation review. We closely monitor and control this process to ensure compliance with our data protection policies.
- **Secure Transmission:** When transmitting documents electronically, we use secure methods to protect the data from unauthorised access during transit.

Cookies

Cookies are small text files that are placed on your computer's hard drive by websites you visit. They are widely used to make websites work more efficiently, as well as to provide information to the owners of the site. Cookies enable web applications to respond to you as an individual by gathering and remembering information about your preferences, such as your language choice or login information.

How We Use Cookies

At PLUS, we utilise cookies primarily for enhancing your experience on our website. Here's how:

- **Customisation and Preferences:** We use cookies to recognise your device and remember any preferences you have set on previous visits, helping our website to respond to you as an individual. This customisation makes your interactions with our site more convenient, for example, by remembering your preference not to be asked to sign in every time you visit.
- **Traffic Log Cookies:** These are used to identify which pages are being used. This helps us analyse data about web page traffic and improve our site accordingly to better suit your needs and expectations. We use this information solely for statistical analysis purposes, after which the data is removed from our system.
- **Site Functionality:** Cookies help us understand how visitors use our website, which enables us to improve and streamline user experiences.

Your Choices Regarding Cookies

Most web browsers automatically accept cookies, but you can usually adjust your browser settings to decline cookies if you prefer. This gives you control over what is stored on your computer and can enhance your privacy and security. However, disabling cookies might prevent you from taking full advantage of our website, as some functionalities such as connection persistence may rely on cookies.

Privacy Assurance

We respect your privacy. The cookies we use are designed to improve your experience on our website without infringing on your privacy. Importantly, we do not use cookies to collect personally identifiable information about you nor for advertising purposes. All the cookie-generated information about your website usage can be anonymised before being used for analytics.

Your Rights Concerning Your Personal Data

As a data subject, you have certain rights under data protection law. We are committed to upholding these rights and ensure that you can exercise them:

Right to Access: You have the right to access information held about you. This includes receiving a copy of the personal data we hold about you and confirming that we are lawfully processing it.

Right to Rectification: You can request that we correct the personal data we hold about you if it is incorrect or incomplete.

Right to Erasure: Under certain conditions, you have the right to request the deletion of your personal data where there is no compelling reason for its continued processing.

Right to Restrict Processing: You have the right to request the suspension of the processing of your personal data in specific cases, such as if you want us to establish its accuracy or the reason for processing it.

Right to Data Portability: Where applicable, you have the right to have the personal data we hold about you transferred to another organisation, or directly to you, in a structured, commonly used, and machine-readable format.

Right to Object: You are entitled to object to our processing of your personal data if there is something about your particular situation which makes you want to object to processing on this ground. You also have the absolute right to object to the processing of your personal data for direct marketing purposes.

Rights Related to Automated Decision Making and Profiling: You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

How to Exercise Your Rights: If you wish to exercise any of the rights set out above, please contact us at [contact information]. No fee is generally required. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights).

Complaints: You have the right to make a complaint at any time to a supervisory authority. We would, however, appreciate the chance to deal with your concerns before you approach the authority so please contact us in the first instance.

Changes to Our Privacy Policy

We may update this privacy policy periodically to reflect changes in our information practices or relevant laws. We encourage you to periodically review this page for the latest information on our privacy practices. This will help you stay informed about how we are protecting your personal data and respecting your rights.

It is important that you read any notifications of privacy policy updates we may send you. Your continued use of our services after any changes to the privacy policy will constitute your acceptance of such changes.

Privacy Policy for Employees

PLUS is committed to respecting and protecting your personal data. This Privacy Policy outlines how we collect, use, store, and protect your personal data, in line with the General Data Protection Regulation (GDPR). We also include within this policy the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Changes to data protection legislation will be monitored and implemented to ensure continued compliance with all requirements.

Data protection principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

1. processing is fair, lawful and transparent
2. data is collected for specific, explicit, and legitimate purposes
3. data collected is adequate, relevant and limited to what is necessary for the purposes of processing
4. data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
5. data is not kept for longer than is necessary for its given purpose
6. data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
7. we comply with the relevant GDPR procedures for international transferring of personal data

Data we collect

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a secure personnel file relating to each employee across our secure servers.

Specifically, we hold the following data:

1. personal details such as full name, home address, email address, phone numbers, date of birth, nationality, gender
2. your CV and CV cover letter, qualifications, details on your education and employment history etc
3. information gathered via the recruitment process such as:

a. references from former employers/educators, further qualifications
b. your id/passport/driving licence as proof of identity with visible photo of you
c. immigration status, right to work documentation
d. criminal record/convictions, DBS checks
e. details relating to pay administration such as National Insurance numbers, bank account details and tax codes
f. details of your next of kin

4. further personal detail 'special category data' such as:
    a. information about your physical or mental health or disability status
    b. information on your race, ethnicity, religion, beliefs or your sexual orientation for equality monitoring
5. information relating to your employment with us, including:
    a. job title and job descriptions
    b. your salary
    c. transaction data including details about payments
    d. your wider terms and conditions of employment
    e. details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
    f. internal and external training modules undertaken and certificates
    g. CCTV footage may be captured during various activities on our courses

It is important that the personal data we hold is accurate and current. Please keep us informed if any personal data given to us changes during the course of the relationship between us and you, your child or pupil.

Collecting your data

You provide several pieces of data to us directly throughout the recruitment process. This may be through email, your online profile or other way of communication.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

The majority of the information we collect from you is required by law, or under the terms of a contract we have with you; however, some details are optional. Whenever we request information, we clearly indicate whether it is mandatory (and outline any potential consequences of not providing it) or optional, allowing you to decide whether to share it.

Purpose and lawful basis for processing

The law on data protection allows us to process your data for certain reasons only.

The purpose of and lawful basis for processing the data include compliance with legal obligations or government/regulatory guidance; recruitment and employment obligations;

meeting our safeguarding obligations; administration and protection of our business as well as protecting your vital interests; in the event of emergency, managing any queries or disputes; our legitimate interests, necessity for contractual fulfilments, and processing of salary.

Special category data:

We carry out processing activities using special category data:

- for the purposes of equal opportunities monitoring
- to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

Failure to provide data

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment, or administer contractual benefits.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of consent, contractual necessity, and legal obligation to process this data.

Who do we share your data with

Employees within our company who have responsibility for recruitment will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processed in line with GDPR.

We may share your data with parties, where it is legally required or necessary for another reason allowed under the data protection law. These kinds of disclosures will only be made when strictly necessary for the purpose.

Some of those third parties may be:

- Local authorities
- Your family or representative (e.g. Next of Kin)
- Auditors

- Central and local government
- Health and social welfare organisations
- Police forces, courts, tribunals
- Financial organisations

Sometimes, we may also use your personal information where:

- You have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interests)

Prior and during your employment, some of your information may be passed to:

- Your line managers
- Head Office staff
- Relevant staff at the host institution
- Group Leaders

This information will include your name, contact details and any other necessary information that may be required.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us. We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

Storing your personal information

Personal data and documentation are stored securely, confidentially, and in compliance with data protection laws to prevent unauthorised access or misuse. An employment file is created and maintained for each staff member, containing information relevant to your role and is used solely for purposes directly related to your employment.

All records are stored within our password-protected system, accessible only to authorised personnel. When necessary, these records may be shared with relevant parties, particularly for safeguarding purposes, in accordance with Data Protection laws.

We will retain your personal information while you are employed by PLUS, whether within our head office or summer schools. Additionally, we may retain certain information after your employment ends, where required by law.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site or certain servers, you are responsible for keeping this

password confidential. We ask you not to share a password with anyone and inform us or change your password if you believe that your personal security may have been compromised.

Retention periods

We only keep your data for as long as we need it for and is required by law.

If your application is not successful and we have not sought consent or you have not provided consent upon our request to keep your data for the purpose of future suitable job vacancies, we will keep your data for six months.

If we have sought your consent to keep your data on file for future job vacancies, and you have provided consent, we will keep your contact details according to the level of consent you have provided. At the end of the relevant time period, we will delete or destroy your data, unless you have already withdrawn your consent to our processing of your data in which case it will be deleted or destroyed upon your withdrawal of consent.

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data and there will be no consequences of withdrawing consent.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. PLUS will retain most of the personal data we have obtained during recruitment and onboarding for up to six months following the end of your contract. This retention period allows for the resolution of any disputes or complaints that may arise during or after the contract term. If, in very exceptional circumstances, it is considered necessary to keep personal data for longer than six months, PLUS will do so in accordance with Data Protection policies and relevant legislation.

We will retain certain types of data for a period of 6 years wherever this is required by HM Revenue and Customs (HMRC). This includes records of employee pay, deductions, reports made to HMRC, payments to HMRC, employee leave and sickness absences, tax code notices, and taxable expenses or benefits.

Your rights

The right to be informed

In order to keep you informed about how we use your data, we have a privacy notice for employees.

The right of access

You have the right to access your personal data which is held by us. You can find out more about how to request access to your data by reading our Subject Access Request policy.

The right to 'correction'

If you discover that the data we hold about you is incorrect or incomplete, you have the right to have the data corrected.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.

You will be informed if we decide not to take any action as a result of the request. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

The right of 'erasure'

In certain circumstances, we are required to delete the data we hold on you. Those circumstances are:

- where it is no longer necessary for us to keep the data;
- where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;
- where you object to the processing (see below) and the Company has no overriding legitimate interest to continue the processing;
- where we have unlawfully processed your data;
- where we are required by law to erase the data.

We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

The right of 'restriction'

You have the right to restrict the processing of your data in certain circumstances.

We will be required to restrict the processing of your personal data in the following circumstances:

- where you tell us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate;
- where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it;

- when the data has been processed unlawfully;
- where we no longer need to process the data but you need the data in relation to a legal claim.

Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.

You will be informed before any restriction is lifted.

The right to data 'portability'

You have the right to obtain the data that we process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.

Data which may be transferred is data which:

- you have provided to us; and
- is processed because you have provided your consent or because it is needed to perform the employment contract between us; and
- is processed by automated means.

We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is two months.
We will not charge you for access to your data for this purpose.

You will be informed if we decide not to take any action as a result of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

The right to 'object'

You have a right to require us to stop processing your data; this is known as data objection.

You may object to processing where it is carried out:

- in relation to the Company's legitimate interests;
- for the performance of a task in the public interest;
- in the exercise of official authority; or
- for profiling purposes.

In some circumstances we will continue to process the data you have objected to. This may occur when:

- we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
- the processing is required in relation to legal claims made by, or against, us.

If the response to your request is that we will take no action, you will be informed of the reasons.

Right not to have automated decisions made about you

You have the right not to have decisions made about you solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you. However, the Company does not make any decisions based on such processes.

Staff Responsibilities

At PLUS, every staff member plays a vital role in upholding our commitment to the highest standards of data privacy and protection. It is imperative that all employees understand their responsibilities regarding the handling of personal data to ensure compliance with the General Data Protection Regulation (GDPR) and our internal data protection policies.

General Responsibilities

- All staff are required to familiarise themselves with and adhere to our data protection policies.
- Staff must handle personal data with utmost care and only access, use, or process such data as necessary for their job functions. Unnecessary or unauthorised access to personal data is strictly prohibited.
- Every staff member is responsible for ensuring the information they collect or manage is accurate and up-to-date. Prompt correction of inaccuracies in personal data is essential, and procedures are in place for regularly verifying and updating data.

Security Practices

- Maintaining the confidentiality and security of personal data is paramount. Staff must follow all specified organisational security measures, such as using strong passwords and handling sensitive information with discretion.
- When transmitting personal data, employees must use secure communication methods provided by the organisation. The sharing of sensitive information over unsecured channels, such as personal email accounts, is prohibited.

- Staff should collect and process only the data that is essential for the specified purpose and avoid unnecessary data collection. This minimisation of data aligns with GDPR principles and reduces the risk of data breaches.

Reporting and Incident Management

- If a staff member suspects that a data breach has occurred or that personal data has been accessed or used improperly, they must report this immediately to the Head Office. We have a formal procedure in place for managing data breaches, including assessment, containment, and remediation activities.
- Employees are expected to cooperate fully with any audits or checks on our data protection processes and compliance. This may involve providing access to data they manage or offering insights into their handling practices.

Disciplinary Actions

Non-compliance with our data protection policies can result in disciplinary action, up to and including termination of employment. Such actions are necessary to maintain trust and integrity within our operations and to mitigate any legal or reputational risks associated with data breaches.