St Giles International:

Data Protection Policy

1. Policy statement

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our students, staff and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 All staff must comply with this policy whenever they are involved in processing personal data. Any breach of this policy may result in disciplinary action.

2. About this policy

2.1 The types of personal data that St Giles International (**We**) may be required to handle include information about current, past and prospective students, current and former staff, homestay hosts and their families or other residents in the home, and other third parties, such as those with whom we communicate. The personal data, which may be held electronically or in structured paper files, is subject to certain legal safeguards specified in the Data Protection Act 1998 and, from 25 May 2018, the General Data Protection Regulation (collectively, the **Data Protection Legislation**).

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from individuals, or that is provided to us by individuals or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied whenever we obtain, handle, process, transfer and store personal data.

2.5 The Managing Director is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Principal of the relevant St Giles International centre and / or the Director of UK Junior courses.

3. Definitions of data protection terms

3.1 **Data** is information which is stored electronically or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controller** is the organisation which determines the purposes for which, and the manner in which, any personal data is processed. A data controller is responsible for establishing practices and policies in line with the Data Protection Legislation. We are the data controller of all personal data used in our business for our own purposes.

3.5 **Data processor** is any organisation that is not an employee that processes personal data on our behalf and on our instructions.

3.6 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.7 **Special categories of personal data** include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life. Special categories of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned. Information relating to the commission of, or proceedings for, any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings is subject to similar safeguards.

4. Data protection principles

4.1 Anyone processing personal data must comply with the data protection principles. These state that personal data must be:

(a) Processed fairly and lawfully

(b) Processed for limited purposes and in an appropriate way

(c) Adequate, relevant and not excessive for the purpose

(d) Accurate and up to date

(e) Not kept longer than necessary for the purpose

(f) Kept secure

4.2 In addition, the Data Protection Legislation requires that personal data must be processed in line with data subjects' rights and not transferred to people or organisations situated in countries without adequate protection.

5. Fair and lawful processing

5.1 The Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed.

5.3 Whenever special categories of personal data or information about criminal offences (such as DBS checks) are being processed, additional conditions must be met.

5.4 When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. Processing for limited purposes

6.1 In the course of our business, we may collect and process the personal data for a variety of purposes, including enrolment of our students, administration of our courses, details of homestays, recruitment of staff and staff administration, and compliance with our legal obligations.

6.2 Personal data may include information we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and information we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, the Disclosure and Barring Service and others).

6.3 We will only process personal data for the specific purposes set out in this policy or for any other purpose permitted by the Data Protection Legislation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter. Further information about how we process personal data relating to our staff is contained in our Staff Handbook.

7. Notifying data subjects

7.1 If we collect personal data directly from data subjects, we provide them with the transparency information required under the Data Protection Legislation. This includes the purpose or

purposes for which we intend to process that personal data, the types of third parties with whom we may share the data and the existence of rights for data subjects.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We will inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. Adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. Accurate data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Timely processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. Processing in line with data subject's rights

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see paragraph 15 for more information).

(b) Prevent the processing of their data for direct-marketing purposes.

11.2 From 25 May 2018, data subjects will have additional rights to request:

(a) That any inaccurate personal data about them is corrected

(b) That their personal data is deleted

(c) That we stop using their personal information for certain purposes

(d) That personal data is provided to them in a portable format

(e) That decisions about them are not made by wholly automated means

11.3 Some of the rights listed above are limited to certain defined circumstances and we may not be able to comply with requests.

11.4 If a data subject is unhappy with the way we are processing or have processed their personal data, they have a right to complain to the Information Commissioner's Office. More information about this can be found at: https://ico.org.uk/concerns/.

12. Data security

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

12.4 Security procedures include:

(a) **Entry controls**. Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment**. All computer users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. Transferring personal data to a country outside the EEA

13.1 We may transfer any personal data we hold to a country outside the European Economic Area (**EEA**), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2 Subject to the requirements listed above, personal data we hold may also be processed by employees operating outside the EEA who work for us or for one of our suppliers.

14. Disclosure and sharing of personal information

14.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

14.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with selected third parties for the purposes set out in this policy.

15. Dealing with requests for exercise of individual rights

15.1 Data subjects may make a request under the rights listed in paragraph 11, including for access to information we hold about them. Employees who receive such a request should forward it to the Principal / Director of Junior Courses immediately.

15.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

15.3 Our employees will refer a request to their line manager [or NAME] for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16. Changes to this policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.