DATA PROTECTION POLICY

Policy Statement

Your privacy is important to us at IH Manchester. We have developed this policy to provide you with information on data we collect, how and why we process it and your rights. We have to collect and use information about students, hosts and staff for the company either on a paid or voluntary basis. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and the hosts, students and staff at IH Manchester and those who we do business with. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function and coordination of our host families as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of students, hosts and staff applicants and existing and former students, hosts and staff. These are referred to in this policy as relevant individuals.

DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is 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.

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:

- processing will be fair, lawful and transparent
- data be collected for specific, explicit, and legitimate purposes
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing

- data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- data is not kept for longer than is necessary for its given purpose
- data will be 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
- we will comply with the relevant GDPR procedures for international transferring of personal data

TYPES OF DATA HELD

HOSTS

We keep several categories of personal data on our hosts in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each host and we also hold the data within our computer system, office 365, which is a secure online share file and complies with all data protection law under GDPR. We also store this data on our secure database, ElsieApp. Only those who require these records for processing and health and wellbeing have access to these records.

Specifically, we hold the following types of data:

- personal details such as name, address, phone numbers
- personal details on people living in the house (lodgers, adult children, partners)
- information gathered via the recruitment process such as past hosting record, references from former employers, details on your employment history.
- details relating to pay administration such as bank account details
- medical or health information
- DBS disclosure of every adult living in the home
- information relating to your hosting with us, including:
    - description of your home (including photos)
    - documents, forms and information supporting your hosting application and your wider terms and conditions of hosting
    - details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings
    - identification documentation
    - dates of last gas safety inspection certificate
    - students' feedback

STAFF

- personal details such as name, address, phone numbers
- information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education, employment history, qualification certificates and proof of right to work.
- details relating to pay administration such as National Insurance numbers, bank account details and tax codes
- medical or health information
- information relating to your employment with us, including:
    - job title and job descriptions

- your salary
- your wider terms and conditions of employment
- 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
- internal; and external training modules undertaken

STUDENTS

- personal details such as name, address, phone numbers, email
- information gathered via the booking process such as school reports, references identification document expiry dates.
- medical or health information including next of kin contact details
- information relating to your programme with us, including:
  - travel dates
  - flight details
  - nationality
  - parents details and consent form where needed (Under 18s)

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice, which is available from the school.

INDIVIDUALS RIGHTS

You have the following rights in relation to the personal data we hold on you:

- the right to be informed about the data we hold on you and what we do with it;
- the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
- the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
- the right to have data deleted in certain circumstances. This is also known as 'erasure';
- the right to restrict the processing of the data;
- the right to transfer the data we hold on you to another party. This is also known as 'portability';
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on data rights under GDPR.

RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems on a regular basis.

LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the hosts consent in order to process data.

We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Hosts will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

ACCESS TO DATA

As stated above, People have a right to access the personal data that we hold on them. To exercise this right, people should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge may be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any individuals benefits operated by third parties;
- disabled individuals - whether any reasonable adjustments are required to assist them at work;
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
- for Statutory Sick Pay purposes;
- HR management and administration - to consider how an individual's health affects their ability to do their job;
- for reasons of accreditation of the school, ensuring smooth and legal processes of administration, adhering with accreditation requirements
- the smooth operation of any employee insurance policies or pension plans;
- to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.
- these kinds of disclosures will only be made when strictly necessary for the purpose.

DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe. IH Manchester have limited their paper records to the maximum.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them. Passwords should not mirror those of personal login to social media sites or personal emails. Passwords should be changed on a regular basis.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary.
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- ensuring that laptops or USB drives are not left where they can be stolen.
- ensuring laptop or device is password protected.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

INTERNATIONAL DATA TRANSFERS

At times, the Company may transfer personal data of host or students to recipients outside of the UK. This transfer will be for means of the performance of the contract between us and the host and to allocate the students to the host family. Where this is required we will ensure we have consent from the host. The Company does not transfer personal data of employees or Students to any recipients outside of the UK. IH Manchester has international transfer of data agreements with agents within the EEA.

Following the UKs exit from the EEA/EU IHM have appointed a GDPR representative within the EU to work with on data requests. IHMs GDPR repetitive in the EEA/EU and contact details are: -

EEA / EU Representative Office	**Italy Office**	**Spain Office**
Attention: Data Protection Officer Telephone: +39 064 520 0328	Gallery Teachers Via costa smeralda, 33 07021 - Arzachena-SS Italy	Gallery Teachers Av. Arquitecto Gómez Cuesta, 16, piso 9-3, 38650 Arona, Santa Cruz de Tenerife Spain

REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

TRAINING

New staff must read and understand the policies on data protection as part of their induction.

All staff receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All staff who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

John O'Leary- Director

john@ihmanchester.com