Data Protection Policy – Organisation

Everyone has rights with regards to how their personal information is handled. During Englishour activities we may collect, store and process personal information about staff, students, guardians, host families, educational partners, clients and service providers, and recognise the need to treat this data in an appropriate and lawful manner. Englishour is committed to complying with its obligations in respect to all personal data it handles.

The types of personal data that Englishour may be required to handle includes details of current, past and prospective employees, students, guardians, educational partners, host families, suppliers, customers and others that Englishour communicates with. The information, which may be held on paper or on a computer or other media is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) (EU) 2016/679 and other regulations. The GDPR impose restrictions on how Englishour may collect and process data.

In accordance with GDPR, Darren Orr is the designated 'Data Protection Lead' (DPL) within Englishour and is responsible for all aspects of the Data Protection Policy and implementation of same.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

Purpose and Scope of the Policy
This policy sets out Englishour's rules on data protection and the legal conditions that must be satisfied in relation to the collection, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information.

If an individual considers that the policy has not been followed in respect of personal data about themselves or others they should raise the matter with the DPL.

Definition of Data Protection Terms
Data – Information which is stored electronically, on a computer, or in certain paper-based filing systems. This includes IT systems and CCTV systems.

Data Subjects - For the purposes of this document includes all living individuals about whom Englishour holds personal data.

Personal Data – Data relating to a living individual who can be identified from the data (or from that data and other information that is in, or likely to come into the possession of the data controller). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers – The individuals or organisations who control and are responsible for keeping and use of data.

Data users – Employees whose work involves using personal data. Data users have a duty to protect the information they handle by following Englishour's data protection security policies at all times.

Processing – Performing any operation or set of operations on data including: -

- Obtaining, recording or keeping data
- Collecting, organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the information or data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blacking, erasing or destroying the data

Sensitive personal data – Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition or sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be: -

a) Obtained and processed fairly

GDPR's are intended not 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. The data subject must be told who the DPL is, in this case Darren Orr, the purpose for which the data is to be processed by Englishour, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions must have been met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

b) Kept only for one or more specified, explicit and lawful purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for other purposes specifically permitted by

GDPR. This means that personal data must not be collected for one purpose and used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. Any employee personal data collected by Englishour is used for ordinary Human Resources purposes. Where there is a need to collect employee data for another purpose, Englishour will notify the employee of this and where it is appropriate will get employee consent to such processing.

c) Used and disclosed only in ways compatible with these purposes

Personal data should only be collected to the extent that it is required for the specific purposes notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

d) Kept safe and secure

Englishour and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

GDPR require Englishour to put in place procedures and technologies to maintain the security of all personal data. Personal data may only be transferred to a third-party data processor if the third party has agreed to comply with those procedures and policies or has adequate security measures in place.

The following must be maintained: -

- Confidentiality – Only people authorised to use the data can access it. Englishour will ensure that only authorised persons have access to an employees' personal file and any other personal or sensitive data held by Englishour. Employees are required to maintain the confidentiality of any data to which they have access.
- Integrity – Personal data is accurate and suitable for the purpose for which it is processed.
- Availability – Only authorised users should be able to access the data if they need it for authorised purposes

Security Policy / Procedures include: -

- Secure lockable desks and cupboards. - Clear desk policy, all desks and cupboards remain locked when not in use. (Personal information is always considered confidential) and treated with extra precautions ensuring no one can see work that contains the same.

- Methods of disposal. – Paper documents must be shredded. All removable media should be wiped and physically destroyed when no longer required.
- Equipment – Data users should ensure that individual monitors do not show confidential information to passers-by and that the screen saver starts as soon as their PC is unattended.
- ISO 27001 – Compliance is required to all Policies with regards to ISO27001, including the IT Security Policy documents.

e) Kept accurate, complete and up to date

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed. Employees should ensure that they notify the DPL and Human Resources of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to data would include a change of address.

f) Adequate, relevant and not excessive

g) Retained for no longer than is necessary for the purpose or purposes for which it was collected

Personal data should not be kept longer than is necessary for the purpose. For guidance in relation to data retention to data retention employees should contact their manager. Englishour has various legal obligations to keep certain employee data for a specified period. In addition, Englishour may need to retain personal data for a period to protect its legitimate interests.

h) Provided to data subjects as requested

Data must be processed in line with data subject's rights. Data subjects have a right to: -

- Request access to any data held about them by the Data Controller
- Prevent the processing of their data for direct marketing purposes
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause or distress to themselves or anyone else

Dealing with Subject Access Requests

A formal request from a data subject for information that Englishour holds about them must be made in writing. Any employee who receives a written request in respect of data held by Englishour should forward it to the Data Controller.

Providing Information Over the telephone

Any employee dealing with telephone enquiries should be careful disclosing any personal information held by Englishour over the phone. The employee should: -

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to their manager and/or the Data Controller for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Direct Marketing

At Englishour, it is our policy not to contact any potential individuals without their permission. To comply with this policy, our pre-sales employees are requested to ensure the following: -

- Do not call or email another organisation until it is confirmed that they have a web presence or already in the public domain with their contact details such as address, and telephone number published on the same.
- When a call is made, permission must be sought to get the correct contact information such as the relevant decision maker with regards to IT purchasing. A record must be kept of whom our employee spoke to and date and time of the call.
- All email contact must contain an 'Opt-Out' clearly identified options.
- We do not market via Postal, Text or Fax.
- All Opt-Outs must be respected (telephone or electronic) by deleting the contact permanently.

Policy Review

Englishour will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required considering changes in the law and organisational or security changes.