DATA PROTECTION POLICY

Colchester English Study Centre and International Language Holidays need to collect and use certain types of information about people with whom it deals in order to operate and deliver services. This includes information of current, past and present employees, students, homestay providers, agents, suppliers and others with whom we communicate.

This information will be dealt with properly however it is collected, recorded and used, be it on paper, electronically or recorded on other material. There are safeguards to ensure this is in line with the Data Protection Act 1998, including shredding/secure destruction of confidential material and ensuring information is kept secure/locked away when not in use.

We regard the lawful handling of personal information by CESC and ilh as very important to maintain confidence between those we deal with and ourselves. We ensure that personal information is treated lawfully and correctly. All staff are required to adhere to the following eight principles of the Data Protection Act 1998, which states that all personal data must:

1. be processed fairly and lawfully
2. be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. be accurate and, where necessary, kept up to date
5. not be kept for longer than is necessary for that purpose or those purposes
6. be processed in accordance with the rights of data subjects under this Act
7. be protected in appropriate ways
8. not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Policy

Colchester English Study Centre and International Language Holidays will:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligation to specify the purposes for which information is used and by whom
- Collect and process appropriate information, only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements, and not disclose information on individuals to third parties without the prior agreement of those individuals (eg references)
- Ensure that personal information is accurate and kept up-to-date
- Retain personal information for 5 years, or for as long as is necessary for legal or operational reasons
- Destroy personal data when no longer required
- Respect the rights of the individual in relation to access of their personal details
- Take appropriate security measures to safeguard personal information
- Ensure that personal information is not transferred outside the European Economic Area without appropriate safeguards

This policy applies to all staff of CESC & ilh, homestay providers, group leaders, contractors & suppliers, volunteers and students.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Responsibilities

Everyone who works for or with CESC and Ilh has some responsibility for ensuring data is collected, stored and handled appropriately.

Each staff member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible that CESC and ilh meet their legal obligations.
- The **Data Protection Officer (Emel Kilickaya)** is responsible for
    - Keeping the Board updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies
    - Dealing with requests from individuals to see the data CESC and ilh hold about them
    - Approving any contracts with third parties that may handle the Company's personal data
    - Arranging data protection training and advice
    - Ensuring all systems services and equipment storing data meet acceptable security standards
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Approving any data protection statements attached to communications such as emails. and letters
    - Addressing any data protection queries from journalists or media outlets
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection
    - Evaluating third-party services the company may use to store or process data

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.
- **CESC and ilh will provide training** to all employees to help them understand their responsibilities when handling data
- Employees should keep data secure, by taking sensible precautions
- Passwords should never be shared with unauthorised persons
- Personal data **should not be** disclosed to unauthorised people, either within the company or externally
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer needed it should be deleted or disposed of
- Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspects of data protection

Data Storage

These rules describe how and where data should be safely stored. Questions relating to the storing of data can be directed to the Data Protection Officer.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data stored electronically but have to be printed for some reason:

- When not required, the paper files should be kept **in a locked drawer or filing cabinet with the keys not left in the lock**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, eg next to a printer
- Data **printouts should be shredded** or if a large number of paper files require disposal, a secure waste bag used which is available from the Data Protection Officer

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by passwords**
- If **data is stored on removable media** it should be kept locked away when not being used
- Servers should be sited away from general office space and **locked**

- Data should never be saved directly on to Laptops, smartphones or other mobile devices **without permission**
- All servers, computers and laptops should be protected **by approved security software and a firewall**

Data use

Personal data is of no value to CESC and ilh unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended
- Personal data **should not be transferred outside the European Economic Area** unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing personal data
- Employees should seek permission from their line managers before saving any personal data to their personal devices. In such cases, devices must be encrypted

Data use

The law requires CESC and ilh to take reasonable steps to ensure data is kept accurate and up to date.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CESC and ilh will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and the company's legal advisers where necessary.

Disclosing data for other reasons

CESC and ilh aim to ensure that individuals are aware that their personal data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

It is the responsibility of all CESC and ilh staff to comply with the Act.

SIGNED _____

PRINT NAME_____

POSITION _____

DATE _____