# Data Protection and Privacy Note

## Table of changes

| Date | Version | Summary of Amendments | Author |
|---|---|---|---|
| 27 Jul 2020 | 1 | n/a | JC |
| 30 Nov 2021 | 2 | Added right to lodge complaint with ICO; Argentina and Japan as data destination; data breach procedure | JC |
| 20 Sep 2022 | 3 | Change to CEE<br>Added specifics relating to DBS checks; Chile as data destination added | JC |

## General

This policy serves as a guide for Cultural Experience England (CEE) to collect, use and store all data fairly, accurately and in accordance with relevant legislation. It ensures the protection of data of students, host families and staff.

This policy has been sent to all current and past host families in the UK. New families will see this policy when they register with CEE. Partners and students are required to acknowledge this policy when applying for a space.

As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, Cultural Experience England Ltd complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

## Relevant Legislation

This policy is based on the requirements stated in the following:

- Data Protection Act 1998
- Freedom of Information Act 2000
- General Data Protection Regulation 2018

Cultural Experience England will review this policy and adapt it to reflect changes in the law when they occur.

# Data Protection and Privacy Note

## Registration with the Information Commissioner's Office

Cultural Experience England Ltd is registered with the Information Commissioner's Office (ICO). The registration is renewed annually.

## Data held by Cultural Experience England

Cultural Experience England collects data from potential host families, students and schools. This includes

- Full legal names
- Date of birth
- Gender
- Professional background
- Address
- Telephone number
- Email address
- Family members, their names and ages
- Contact details for students' parents
- Medical information, medication
- Nationality and right to work in the UK (host families and staff only; can include passport picotee page or ID document data)
- DBS certificate number, date of issue (host families and staff; older students in shared accommodation) and contents
- Contact details for schools
- Names and positions of contact persons in schools

All data must be accurate and kept up to date. Staff are to update all databases as soon as they learn of a change.

## Data sharing and use

CEE collects data from potential host families and students. CEE only shares data for the purpose of student visits and only shares as noted below:

- Student data is shared with potential host families to allow them to choose.
- Host family data is shared with potential students.

- After student and host family have been matched, this data is shared with the partner organisation.
- Student and host family data are shared within CEE.
- Some student data is shared with schools, as are the name and contact details of the host family.
- Data about the student and host family is shared with social services when a student under 16 is placed. Social services may share data with CEE if there are medical or safeguarding concerns.
- Data will be shared with authorities such as police or hospitals in the event of a medical emergency, a student having gone missing or a crime, if the authorities have a legitimate interest in the data.
- Contact details for host families, natural families, partner organisations and schools are shared with our accrediting body AEGIS (Association for the Education and Guardianship of International Students, The Wheelhouse, Bond's Mill Estate, Bristol Road, Stonehouse, Gloucestershire GL10 3RF, www.aegisuk.net) for the purposes of CEE's accreditation and reaccreditation only. AEGIS will store the data in a safe way and delete them when (re)accreditation is complete.
- In accordance with section 124 of the Police Act 1997, DBS certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information have been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it. The record is kept in CEE's account on the secure webportal ukcrbs.co.uk; in form of initials on CEE's Zoho database and on the Staff SCR of CEE's affiliate, Brighton International School.
- DBS Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

## Data retention, storage and protection

Cultural Experience England: CEE stores family and student information for a maximum of 10 years. Staff information will be kept for the duration of the employment and for a maximum of six years thereafter.

Data is stored on Zoho Creator and on Google Drive. There are no files or storage on any other software. Both platforms (Zoho and Google) are technically secure and GDPR compliant. Google Drive Data is only shared with CEE staff. Some data about host family initial and annual visits is kept on paper in a locked cabinet.

Where data is shared with partner organisations, students, host families or schools, this is done using G Suite for Business. G Suite is technically secure and GDPR compliant. Recipients of messages are asked never to download personal data to their computers or devices.

All staff agree to be bound by data protection legislation. Downloading student or host family data onto computers and devices is not allowed. All information is accessed on the safe Drive only.

DBS certificate information: Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary and for a maximum of 6 months. This retention will allow for the consideration and resolution of any disputes or complaints or be for the purpose of completing safeguarding audits.
Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.
Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding or electronic deletion. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or electronic trash bin).
We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken. Where a DBS certificate has an entry, a risk assessment will be made. The risk assessment result will be kept on file, not, however, the details of the convictions taken into account.

Host Families*:* Host families are required to delete all student data if the student is not coming to stay with them or after the student has left. Downloads are not permitted. Host families commit to not sharing student data. CEE will send student files only to host families who have acknowledged our GDPR commitment and whose acknowledgement is stored on Zoho database.

Students: Students commit to not sharing or downloading host family data and to deleting or destroying it once it is no longer needed.

Partner organisations: All our partner organisations are in the EEA, Argentina, Chile or Japan and bound by GDPR legislation or equivalent. Each partner organisation is responsible for ensuring data protection with their students and natural families. They acknowledge this policy each time they sign up a student with us.

Schools, Social Services, authorities: Each of these organisations is bound by GDPR legislation and has their own policy which we expect them to follow.

## Data breaches

If a breach in data protection occurs accidentally or knowingly, CEE will contain it, record it and assess the risk to the data subjects concerned. Factors to be considered are the number of data subjects impacted, the volume of breached data per individual, the likelihood of adverse consequences for the subjects, the severity of the adverse consequence for the subject Where there is a negligible risk, the breach will be dealt with internally. If a risk to the freedom and rights of the data subject is likely, the

breach will be notified to the ICO. Whenever there is a high risk of the data subject being impacted, CEE will inform the data subject of the breach and the subsequent actions taken to contain it.

## Your rights

Data subjects have the right to request a report of any of their data held or shared at any point. Data deletion can be requested. Consent to have data collected and stored can be withdrawn at any point and confirmation of such will be sent within 24 hours. Data subjects can request to have their data updated or rectified if wrong. Complaints can be directed to CEE and / or the Information Controller's Office (ICO).