Data Protection Policy

Introduction

As part of the general management and administration of our business, Centre of English Studies will at certain times create and obtain data relating to finances, holdings, clients, staff and business arrangements. It is vital that all such data collection, management and storage be handled in a manner that adheres to relevant laws and charters (see links below) and reflects CES commitment to corporate responsibility in this area.

It is essential that we assert and protect the fundamental privacy rights of individuals in the collection and use of all personal data. Data protection must strike a balance between those individual rights and the legitimate business of CES in relation to such.

CES is not of sufficient scale that a Data Protection Office DPO is appropriate. In each team – Admin, Finances, Marketing and Academic, the manager will be responsible reporting to the CEO Justin Quinn. Record keeping, documentation, processes, audits and reviews must demonstrate adherence to CES policies and accountability in this regard.

Purpose of the policy

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR). It will apply to all information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Personal Data

Personal Data in our context refers to items such as:

Name, age, location data, online identifiers, qualifications, background information, factors relating to the physiological, mental, genetic, socio-economic, financial, gender identification, health, cultural and social identity of the individuals.

We will be required to store and to process data about:

- current, past and prospective students
- current and former staff
- homestay hosts and their families including other residents in their homes

Every effort will be taken to ensure that the collection of data in relation to the above is limited to that necessary for CES to perform efficiently in the following explicit and legitimate areas:

- the functions of arranging student accommodation and transfers,
- classes, examinations and academic record keeping,
- financial operations and invoicing
- recruitment and staffing

Definition of Terms

- **Data subject –** all living individuals about whom we hold data
- **Data –** any stored information (whether electronic or paper)
- **Personal data** – data relating to a living individual who can be identified from that data. It can be factual or opinion based. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- **Special categories of personal data** – this would include information about a person's racial or ethnic origin, political opinions, religious beliefs, physical health, mental health, sexual orientation, criminal record. ***The processing of such data may only be done under strict conditions and requires the explicit and informed consent of the individual concerned. Please see below.***
- **Data controller** - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed
- **Data processor** - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
- **Processing** - in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
- a) organisation, adaptation or alteration of the information or data,
- b) retrieval, consultation or use of the information or data,
- c) disclosure of the information or data by transmission, dissemination or otherwise making it available to a third party

Data Protection Principles

CES will adhere to the following basic principles of data protection

- Lawful Processing:

- Individual has given consent for the use of their data for one or more specific purposes
- Processing is necessary for the performance of a contract between CES and the individual/organisation
- Processing is necessary for compliance with CES compliance with legal obligations
- Processing is necessary to protect the vital interests of the individual

- Purpose Limitation & Data Minimisation:

- The use of data collected for these purposes should be limited to that particular purpose.
- Where student data is requested for marketing purposes, written permission will be obtained first. Lack of response/no visible objection will not be taken as consent.

- Accuracy:

- Every reasonable effort should be taken that personal data be accurate and up to date.

- Storage Limitation:

- Data must be kept in an identifiable form for no longer than necessary. Please see Document Retention outlines below.

- Integrity and Confidentiality:

- Data should be processed and stored in a manner that retains its confidentiality, protects against theft, unlawful processing, accidental loss, destruction or damage.

Lawful basis for processing data

Consent – We will use this lawful basis if an individual has freely and explicitly given their written consent for us to do so.

Contract – We will use this lawful basis if we need to process your personal data: to fulfil our contractual obligations to the person in question.

Legal obligation – We will use this lawful basis if we need to process the personal data to comply with a common law or statutory obligation.

Vital interest - We will use this lawful basis if we need to process the personal data to protect someone's life.

Legitimate interest – We will use lawful basis where identify a legitimate interest and show that the processing is necessary to achieve it; and balance it against the individual's interests, rights and freedoms. The legitimate interests can be our own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

Processing special category data

Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In order to lawfully process special category data, we will identify both a lawful basis and a separate condition for processing special category. These do not have to be linked. There are ten conditions for processing special category data in the GDPR. We will select a lawful basis from the list above and one from the following list in order to process this type of data:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Notifying data subjects of our activities

We set out clearly in our Privacy Notice which is on our website, and available in paper form upon request, for what purpose we are collecting their data, on what lawful basis and whether or not we intend to pass their data to any third parties. We ensure that our Privacy Notice is:

- Concise, transparent, intelligible and easily accessible
- Written in clear, plain language (especially if you're addressing children)
- Available free of charge

Consent forms also provide information to our data subjects in line with GDPR requirements. This policy is also be available on our website and will be emailed on request.

Rights of data subjects

Right to be informed - Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We will provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. This is called 'privacy information'. We will provide privacy information to individuals at the time we collect their personal data from them. If we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of

obtaining the data and no later than one month. The information we provide to people will be concise, transparent, intelligible, easily accessible, and it will use clear and plain language. We will bring any new uses of an individual's personal data to their attention before we start the processing.

Right of access - Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. **If data subjects want access to their data, in the first instance they should contact the principal of the school in which they are studying**

Right of rectification of data - The GDPR gives individuals the right to have personal data rectified. Personal data will be rectified if it is inaccurate or incomplete.

Right to erasure - The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child

Right to restriction - Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future. We will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Right to portability - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Data security

We will take all reasonable measures to store data securely, whether in electronic form or paper form.

Data Breach

- A personal data breach is defined as:

  a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Upon becoming aware of any such breach, notification must be made to the relevant Data Protection Commissioner (see links below), no later than 72 hours.

- Report should be made by the local Data Compliance Officer and must identify the likely consequences of the breach and the measures taken/to be taken to mitigate possible adverse effects for individuals. See Appendix 2 below for **Breach Notification Form** and further details.

- Facts surrounding the breach, its effects, remedial action taken must be documented to verify compliance.

- Individuals must be notified if the breach is likely to result in high risk for their rights and freedoms

Practical Considerations

- CES operates a Clean Desk Policy. All documents of a sensitive/restricted or personal nature are to be tidied away and either securely disposed of or locked away when the workspace is not occupied. This includes Post-Its and memos.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- All CES computers are timed to lock automatically at 5 minutes. All CES computers require a password to access.
- Those leaving their desk or workspace are required to manually lock their computer as follows:
    - Press the Win+L key combination on the computer keyboard (Win is the Windows key and features the Windows logo).
    - Click the padlock button in the lower-right corner of the Start button menu to lock your PC.
- Computer workstations must be shut down at the end of the day.

Appendix 1

Document Retention by Years

1 YEAR

Correspondence with Customers and Vendors
Duplicate Deposit Slips
Purchase Orders (other than Purchasing Department copy)
Receiving Sheets
Requisitions
Stenographer's Notebooks
Stockroom Withdrawal Forms

3 YEARS

Class/academic records
Employee Personnel Records (after termination)
Employment Applications
Expired Insurance Policies
General Correspondence
Internal Audit Reports
Internal Reports
Petty Cash Vouchers
Physical Inventory Tags
Savings Bond Registration Records of Employees
Time Cards For Hourly Employees

6 YEARS

Accident Reports, Claims
Accounts Payable Ledgers and Schedules
Accounts Receivable Ledgers and Schedules
Bank Statements and Reconciliations
Cancelled Checks
Cancelled Stock and Bond Certificates
Employment Tax Records
Expense Analysis and Expense Distribution Schedules
Expired Contracts, Leases
Expired Option Records
Inventories of Products, Materials, Supplies
Invoices to Customers
Notes Receivable Ledgers, Schedules
Payroll Records and Summaries, including payment to pensioners
Plant Cost Ledgers
Purchasing Department Copies of Purchase Orders
Sales Records
Subsidiary Ledgers
Time Books
Travel and Entertainment Records
Vouchers for Payments to Vendors, Employees, etc.
Voucher Register, Schedules

FOREVER

Audit Reports from CPAs/Accountants
Cancelled Checks for Important Payments (especially tax payments)
Cash Books, Charts of Accounts
Contracts, Leases Currently in Effect
Corporate Documents (incorporation, charter, by-laws, etc.)
Documents substantiating fixed asset additions

Deeds
Depreciation Schedules
Financial Statements (Year End)
General and Private Ledgers, Year End Trial Balances
Insurance Records, Current Accident Reports, Claims, Policies
Investment Trade Confirmations
IRS Revenue Agents. Reports
Journals
Legal Records, Correspondence and Other Important Matters
Minutes Books of Directors and Stockholders
Mortgages, Bills of Sale
Property Appraisals by Outside Appraisers
Property Records
Retirement and Pension Records
Tax Returns and Worksheets
Trademark and Patent Registrations

Digital academic records

Digital records of certification and examination results

Appendix 2

PRIVACY NOTICE FOR STAFF AND HOMESTAY HOSTS

YOUR PERSONAL INFORMATION AND HOW WE USE IT

Centre of English Studies will collect and use personal information about you (our staff and homestay hosts). We do this through the completion of various forms which ask for your personal details

We hold and use your information to help us fulfil our contractual obligations to you (i.e.to pay you) and to help us provide a safe and secure environment for you to work in. We also use the information in order to ensure that we all have a safe and secure environment for our students (i.e. by asking you to undertake DBS checks)

The information we hold includes (but is not necessarily limited to) your

- personal contact details
- banking details
- evidence of DBS clearance
- information about your family home (in the case of homestay hosts)
- educational qualifications

We will hold all of your personal information securely and only those with a legitimate need to access it will be permitted to. We will not pass any personal information on to third parties unless we have received your **explicit written consent** to do so.

You can ask to see any information we hold about you.

There is no cost to see this information

You can see the full CES Data Protection Policy here by looking on our website or by contacting the Principal

If you have any questions about the way we use your personal data, contact datauk@ces-schools.com

PRIVACY NOTICE FOR STUDENTS

YOUR PERSONAL INFORMATION AND HOW WE USE IT

Centre of English Studies will collect and use personal information about you (our students). We will ask you to complete forms giving us your personal details in case there is an emergency and we need to contact you or someone in your family.

We hold and use your information to help you study and learn, to check and to report on how well you are doing and to make sure you are happy and safe with us.

The information we hold includes your

- contact details
- attendance information
- special educational needs and
- any important medical information

We will give important medical information to your homestay host and to other CES staff members.

We will also give your contact details to homestay hosts and to other CES staff members. We do this for your health and for your safety.

You can ask to see any information we hold about you. Just ask the Principal where you study

There is no cost to see this information

If you want to see our full Data Protection Policy please look on our website or ask the Principal of your school

If you have any questions about the way we use your personal data, contact datauk@ces-schools.com

Appendix 3

LINKS

GDPR Regulation EU 2016/679 - http://www.eugdpr.org/

(GDPR Regulation EU 2016/679 comes into effect 25 May 2018 and repeals and replaces all existing laws.)

Data Protection Act 2017 - https://www.gov.uk/government/collections/data-protection-bill-2017

Data Protection Commissioner (UK) www.ico.org.uk

Data Protection Commissioner (IE) www.dataprotection.ie

GDPR Information (Ireland) www.gdprandyou.ie

Appendix 4

Data Breach Notification Form

How to complete this form:

This Form is in two sections. Section 1 covers the initial information which must be notified to this Office in respect of a data security breach, and Section 2 requests more detailed further information.

A first notification must be made to this Office on this form no later than 24 hours after the first detection of the data breach.

If you have all the information to hand at this stage, you may fill out both sections 1 and 2 of the form.

If you do not have all the necessary information to hand at the time of the first notification, a second notification must be made within 3 days of the first notification, on section 2 of the form. For security purposes, you will not be presented with the information previously supplied in Section 1. When submitting a second notification, please complete Questions 1-3 again and Questions 4-8 if there is any change to the information. If there is no change to your responses to questions 4 to 8 from your initial notification, simply enter "as initial notification".

If at the end of the 3 days, you still do not have all the information required, you must provide as much information as is available and contact:

Ireland: the Data Breach Section of the Office of the Data Protection Commissioner to provide a reasoned justification for the late notification of the remaining information. The Breach section can be contacted on (057) 8684800.

UK: the Data Breach Section of the Information Commissioner's Office. The Breach section can be contacted on 0303 123 1113. The relevant web site may be accessed via https://ico.org.uk/for-organisations/report-a-breach/

SECTION 1

Information in this section is for an initial notification. Preliminary information is sufficient for answers in this section.

Questions 1 and 2

1. Name of the provider and
2. Contact details as indicated.

Question 3

Please indicate whether or not you are making a first or second notification.

You will receive a reference number from this Office when you make your first notification. If you are subsequently making a second notification, please include the reference number here.

Question 4

Please indicate both the date and time when the incident took place and the date and time when the incident was detected by the provider.

Question 5

Please indicate the circumstances surrounding the breach.

Question 6

Please indicate the nature and content of the personal data

Question 7

Please indicate the technical and organisational measures you are applying to secure the affected data.

Question 8

Please indicate if you use other providers to deliver part of the electronic communications service to your subscribers. If the breach was related to the service provided by these other providers, please indicate if they notified you of the data security breach.

At the end of Section 1 you will be given an option either to submit the form as an initial notification or to proceed to section 2 to make a full notification, if you have the information available to you at this time.

If you submit you will receive an automated email as an initial acknowledgment.

SECTION 2

Further Information on the data breach.

Question 9

Please give a summary of the incident that caused the data breach, including the physical location and the storage media involved.

Question 10

Please indicate the number of subscribers or individuals concerned.

Question 11

Please describe the potential consequences and potential adverse effects on subscribers/individuals.

Question 12

Please describe what action you have taken to help mitigate any potential adverse affects to the affected individuals.

Possible additional notification to subscribers/individuals

Question 13

If you have already notified subscribers/individuals, please give the content of the notification.

Question 14

If you have already notified subscribers/individuals, please indicate the means used to notify the breach to subscribers/individuals (e.g. individual notifications- email, letter or phone call, media announcements etc)

Question 15

Please indicate the number of subscribers/individuals notified.

Possible cross-border issues

Question 16

Please indicate if the breach has involved subscribers/individuals in other Member States

Question 17

Please indicate if you have notified other competent national authorities.

If you have notified other competent national authorities, please indicate which authorities you have notified.