

## DATA PROTECTION POLICY - GDPR

### Rationale

European College of law and Business (ECLB) is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how the centres manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the centre will need to be aware of as data controllers, including provisions intended to enhance the protection of student's personal data. For example, the GDPR requires that the College privacy notices are written in a clear and plain language so that the staff and students will understand easily.

ECLB needs to process certain information about its staff, students and other individuals with whom it has a relationship for various purposes such as

1. The recruitment and payment of staff
2. The management of the courses
3. Student enrolment
4. Assessments, internal and external verifications
5. Recording student attendance, assessments of course work and progress
6. Collecting fees
7. Financial compliances and obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR), ECLB must ensure that all this information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

## **Compliance**

This policy applies to all staff and students of ECLB. Any breach of this policy or of the Regulation itself will be considered an offence and the centre's disciplinary procedures will be invoked. As a matter of best practice, other agencies and individuals working with ECLB and who have access to personal information, will be expected to read and comply with this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislations.

## **Our Commitment**

ECLB is fully compliant with GDPR. The institution is committed to ensuring the security and protection of the personal information that we possess, and to provide a compliant and consistent approach to data protection. We have a robust and effective data protection programme in place, which complies with existing law and abides by the data protection principles. We fulfilled our obligations as required to meet the demands of the GDPR Act 2018.

ECLB is dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for this Regulation.

## **General Data Protection Regulation (GDPR)**

This piece of legislation comes into effect on the 25<sup>th</sup> May 2018. it regulates the processing of personal data, and protects the rights and privacy of all living individuals, by giving all individuals a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The GDPR also sets out specific rights for students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Pupil Information) (England) Regulations 2000'. For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website ([www.ico.org.uk](http://www.ico.org.uk)).

## **Responsibilities under the GDPR**

ECLB will be the ‘data controller’ under the terms of the legislation. This means it is ultimately responsible for controlling the use and processing of the personal data. The Principal will address any concerns regarding the data held by the College and how it is processed, held and used.

The Senior Management is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the centre.

The Senior Management is also responsible for ensuring that the College’s notification is kept accurate. Compliance with the legislation is the personal responsibility of all members of the College who process personal information.

Individuals who provide personal data to the College are responsible to ensure that the information is accurate and up-to-date.

## **Data Protection Principles**

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found in the DPCoP. Please follow this link to the ICO’s website ([www.ico.org.uk](http://www.ico.org.uk)).

In order to comply with its obligations, ECLB undertaken to adhere to the following eight principles:

### *1. Personal information must be fairly and lawfully processed*

ECLB will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

## *2. Personal information must be processed for limited purposes*

ECLB will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

## *3. Personal information must be adequate, relevant and not excessive*

ECLB will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

## *4. Personal information must be accurate and up to date*

ECLB will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the centre if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the centre to ensure that any notification regarding the change is noted and acted on.

## *5. Personal information must not be kept for longer than is necessary*

ECLB undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the College will undertake a regular review of the information held.

ECLB will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

## *6. Personal information must be processed in line with the data subjects' rights*

Individuals have various rights under the legislation including a right to:

- be told the nature of the information (eg: enrollment form, proof of identity /address/ qualifications etc) the centre holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision making process that will significantly affect them.

- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

ECLB will only process personal data in accordance with individuals' rights.

### *7. Personal information must be secure*

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

ECLB will ensure that all personal data is accessible only to those who have a valid reason for using it.

ECLB will have in place appropriate security measures such as

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screensaver being used.
- keys held securely in a key cabinet with controlled access

In addition, ECLB will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically.

This policy also applies to staff who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

*8. Personal information must not be transferred to other countries without adequate protection*

ECLB will not transfer data to such countries other than the European Economic Area (EEA) countries without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so ECLB will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the College collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

**Consent as a basis for processing**

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when ECLB is processing any sensitive data, as defined by the legislation.

ECLB understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

ECLB will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

ECLB has a data consent form which is duly agreed and signed by staff and students as a part of GDPR compliance (Appendix 1).

## **Subject Access Rights (SARs)**

Individuals have a right to access any personal data relating to them which are held by the centre. Any individual wishing to exercise this right should apply in writing to the Principal. Any member of staff receiving a SAR should forward this to the Principal.

The centre reserves the right to charge a fee for data subject access requests (currently £20). Under the terms of the legislation, any such requests must be complied with within 40 days.

## **Disclosure of Data**

Only disclosures which have been management approved must be made and therefore staff and students should exercise caution when asked to disclose personal data held on another individual or third party.

ECLB undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the OIC and is in the legitimate interests of the centre.
- the disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.

## **Publication of centre Information**

ECLB publishes various items which might include some personal data, e.g. event information, photos and information in marketing materials etc.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted centre access only. Therefore it is ECLB policy to offer an opportunity to opt-out of the publication of such when collecting the information.

## **Email**

It is the policy of ECLB to ensure that senders and recipients of email are made aware that under the DPA, 2019 and Freedom of Information Act 2000, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the centre's email.

## **Procedure for review**

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 2018.

For help or advice on any data protection or freedom of information issues, please contact ECLB office.