Data Protection Policy
(Version:4)

Elizabeth School of London
Lower Ground Floor
221 Marsh Wall
Moorfoot House,
Meridian Gate
E14 9FJ

Table of Contents

Aim

The Elizabeth School of London operates processes to prevent, identify, investigate and respond to unacceptable academic practice as well as ensures the data are managed as per guidance to meet the expectation of different stakeholders. Besides, we have a commitment to equity in enabling learner development and achievement and providing the security of the information provided to ESL. On the top, we practice code of ethics. These principles give rise to ESL further essential committed to compliance with the requirements of the Data Protection Act 1998 and 2018.

Elizabeth School of London is fully committed to prepare for and, after 25 May 2018, to comply with the General Data Protection Regulation (GDPR). The GDPR applies to all Colleges that process data relating to their employees, as well as to others including students, customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed. We aim to ensure that all staffs, agents, consultants, students and other stakeholders who have access to any personal data, will abide by their duties and responsibilities under the above Acts.

Why this policy exists

This data protection policy ensures:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, students and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Based on the Data Protection Act 2018:

"Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage."

The Principles of Data Protection

Our personnel concerned must comply with the following principles, which are legally enforceable:

- To handle personal and sensitive (about ethnic origin, political opinion, faith, disability, sexual preference, criminal convictions etc.) data fairly and lawfully.
- To be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

- To use personal and sensitive data for specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes.

To use the personal and sensitive data, which are reasonable, relevant and not excessive to that particular purpose.

- Use personal and sensitive data accurately and where necessary, update it

- Keep and protect these personal and sensitive data with an appropriate degree of security.
- Store personal and sensitive data for longer than is necessary for that purpose.
- Any personal and sensitive data would not be transferred outside the UK, unless the recipient authorities ensure an adequate level of data protection.
- These personal and sensitive data will be released either with the person's consent, or for purpose of the national security.
- Adequate, relevant and not excessive - Data collected must be enough to complete the required task and no more.
- Not kept longer than is necessary - personal information should only be retained by the College for as long as is required to fulfil the purposes for which it was originally provided or required by law to be held. Beyond this point it should be securely destroyed.

Data Security:

All staff and students are responsible for ensuring that:

Any personal data, which they process, is kept securely in accordance with the College's Policy;

Personal information is not disclosed accidentally or otherwise to any unauthorised third party.

Employees should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

What Does the Act Mean for Learners?

All learners at the ESL who handle or process personal data about individuals (names, contact detail s,financial details, course details, personal circumstances, beliefs etc) in the course of their studies m ust be aware of the GDPR Principles and how to apply them lawfully within the confines of the Colleg ee General Data Protection Regulation policy.

Student Obligations

Students must ensure that

- All personal data provided to the Elizabeth School is accurate and up to date.
- They must ensure that changes of address etc. are updated on the student registration system.

Sanction

ESL is registered with Commissioner's Office (**ICO**). This policy is applicable for all staffs, students, external personnel and all stakeholders. The Designated Data Protection Officer (DPO) will deal with day-to-day matters. Any member of employees, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the DPO. HR manager will supervise this at all time. Unjustified breach of this policy and misuse of personal and sensitive data may cause instant disciplinary action, dismissal and/or prosecution.