Policy Name: **ICE Data Protection Policy**

Policy Statement:

Irish College of English is committed to a policy of protecting the rights of individuals with respect to the processing of their personal data.
This Policy and the further School guidance it refers to apply to all personal data processed for the school's purposes, regardless of where it is held and, in respect of automatically processed data, the ownership of the equipment used.

Responsible Person: Deirdre Rochford – General Manager and Data Protection Officer

PURPOSE

This document sets out The Irish College of English policy on data protection. It provides an overview of data protection requirements and directs you to more detailed guidance as appropriate.

BACKGROUND TO THIS POLICY

In brief the General Data Protection Regulation (GDPR), establishes a framework of rights and duties which are designed to safeguard personal data. These are referred to in this policy as 'Data Protection legislation'. The legislation is underpinned by a set of six straightforward principles, which define how data can be legally processed.
These six principles are:

- Personal data shall be processed fairly, lawfully and
- Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes. There is an exemption for research
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is
- Personal data shall be accurate and where necessary kept up to
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. There is an exemption for research
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.

The GDPR also sets out rights of data subjects relating to their personal data. These rights include:

- the right to access
- the right to rectification
- the right to erasure (in certain circumstances)
- the right to stop processing
- the right to portability (in certain circumstances)
- the right to object to marketing. and
- the right to have human intervention with regards to automated processing, including profiling

POLICY AND GUIDANCE

APPLICATION OF THIS POLICY

The school holds personal information about individuals such as employees, students, graduates, research subjects and others, defined as **data subjects** in Data Protection legislation. Such data must only be processed in accordance with the Data Protection legislation. This Policy and the School Guidance are written to ensure such compliance. Any breach of this Policy and/or the School Guidance may result in the School as the **Data Protection Officer** (and in some cases individuals), being in breach of Data Protection legislation and therefore liable in law for the consequences of such breach.

All staff are responsible for ensuring that the school complies with Data Protection legislation. All students and staff must ensure they have read and understand this Policy and the School Guidance.

It is the responsibility of all users of personal data throughout the school to ensure that personal data is kept securely. Personal data should not be disclosed to any unauthorised third party in any form, either accidentally or otherwise.

Any breach of or failure to comply with this Policy or the School Guidance, particularly any deliberate release of personal data to an unauthorised third party, may result in disciplinary or other appropriate action.

The School Will continue to perform periodic audits to ensure compliance with this Policy and Data Protection legislation and to ensure that all guidance and support is kept up to date. Any unauthorised access to or disclosure of personal data or other data security breaches should be reported to the Data Protection Officer and/or the Information Security Manager as soon as possible.

The Academic Manager is responsible for ensuring that the school community remain informed of their obligations under Data Protection legislation, with operational duties of advice and support devolved to the Data Protection Officer.

The Data Protection Officer is required by Data Protection legislation to report to the highest levels of management at the school.

Staff procuring cloud-based services or mobile apps storing personal data for the school must check with the Information Security team that these meet the security requirements of Data Protection legislation.

ACCESS TO DATA

The DPO gives data subjects a right to access to personal data held about them within a set timescale. Therefore, it is important that the Data Protection Officer be notified of any request to the school for access to an individual's personal data as soon as they are received.

If you have any questions relating to access to personal data, please contact the Data Protection Officer.

RETENTION OF DATA

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. The school's retention schedule outlines the length of time various classes of records and other data should be kept. This extends to backups and copies made on removable media.

This does not apply to research related data which can be kept indefinitely.

DATA TRANSFER

We put in place safeguards for data that is being sent outside the European Economic Area by the school.

Information published on the web must be considered to be an export of data outside the EEA

INFORMATION ASSET REGISTER

The School's Information Asset Register (IAR) will be used to meet the record keeping requirements of Data Protection legislation.

Information Asset Owners, defined as the staff member with responsibility for the information asset, will ensure that they create and maintain the data held within the Information Asset Register.

This will include an annual review of their information assets.

The Data Protection Officer will ensure that Information Asset Owners receive the appropriate support to maintain the information asset register.

COMPLIANCE, POLICY AWARENESS AND DISCIPLINARY PROCEDURES

The loss or breach of confidentiality of personal data is an infringement of Data Protection legislation and may result in criminal or civil action against LSE. Therefore, all users of personal data at the school's information systems must adhere to the Data Protection Policy and its supporting policies as well as the Information Security Policy.

All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

Any breach of this policy will be handled in accordance with all relevant School policies.